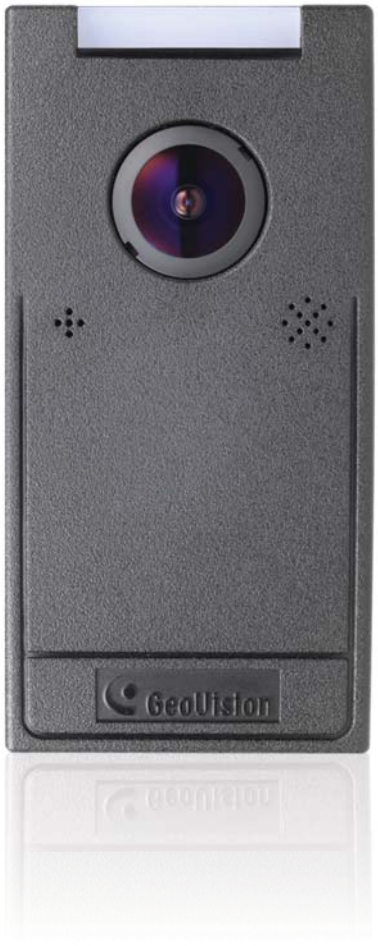
GeoVision inc
The Vision of Security

GV-Camera Reader

GV-CR420 User's Manual



Before attempting to connect or operate this product, please read these instructions carefully and save this manual for future use.

CR420V101-A

© 2013 GeoVision, Inc. All rights reserved.
Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and GV series products are trademarks of GeoVision, Inc. *Windows* and *Windows XP* are registered trademarks of Microsoft Corporation.

February 2013

Contents

Naming and Definition v

Chapter 1 Introduction 1

1.1 Key Features 3
1.2 Packing List 4
1.3 Optional Accessories 4
1.4 System Requirements 5
1.5 Limitations and Optimal Installation for Face Detection 6
1.6 Physical Description 7
1.7 Connecting the Cables and Wires 8
1.8 Installation 9

Chapter 2 Access Control Configurations 11

2.1 Connecting to GV-AS Controller 12
2.1.1 Through Wiegand Interface 13
2.1.2 Through RS-485 Interface 15
2.1.3 Through Network Connection 17
2.2 Setting Up GV-ASManager 19
2.2.1 Adding GV-AS Controller 19
2.2.2 Setting Up Access Control Schedule 21
2.2.3 Receiving Live View from Camera Reader 23

Chapter 3 Establishing Network Connection 25

3.1 Checking the Dynamic IP Address 26
3.2 Assigning an IP Address 28

Chapter 4 Accessing the Camera Reader 30

4.1 Accessing Your Surveillance Images 30
4.2 Functions Featured on the Main Page 31
4.2.1 The Live View Window 32
4.2.2 The Control Panel of the Live View Window 34
4.2.3 Snapshot of a Live Video 37

4.2.4 Video Recording 37
4.2.5 Picture-in-Picture and Picture-and-Picture View....38
4.2.6 Alarm Notification....40
4.2.7 Video and Audio Configuration 42
4.2.8 Remote Configuration 43
4.2.9 Camera Name Display....43
4.2.10 Image Enhancement....43
4.2.11 Network Status 44

Chapter 5 Administrator Mode 45

5.1 Video & Motion 47
5.1.1 Video Settings 48
5.1.2 Motion Detection....52
5.1.3 Privacy Mask 53
5.1.4 Text Overlay 54
5.1.5 Tampering Alarm 55
5.2 Events & Alerts 56
5.2.1 E-mail 56
5.2.2 FTP....58
5.2.3 Center V2 60
5.2.4 VSM....62
5.2.5 Video Gateway / Recording Server 64
5.2.6 RTSP....66
5.3 Monitoring....67
5.4 Network 68
5.4.1 LAN 68
5.4.2 Advanced TCP/IP 70
5.4.3 IP Filtering 73
5.4.4 SNMP Setting 74
5.5 Management....75
5.5.1 Date and Time Settings 75
5.5.2 GPS Maps Settings 77
5.5.3 User Account 79
5.5.4 Log Information....80
5.5.5 Tools....81

Chapter 6 Advanced Applications 83
6.1 Upgrading System Firmware.....83
6.1.1 Using the Web Interface 84
6.1.2 Using the IP Device Utility.....85
6.2 Backing Up and Restoring Settings.....87
6.2.1 Backing Up the Settings.....87
6.2.2 Restoring the Settings.....88
6.3 Restoring to Factory Default Settings.....89
6.4 Verifying Watermark 90
6.4.1 Accessing AVI Files 90
6.4.2 Running Watermark Proof 90
6.4.3 The Watermark Proof Window 91

Chapter 7 DVR Configurations 92
7.1 Accessing Camera View 94
7.1.1 Customizing the Basic Settings.....97
7.2 Receiving Card Numbers on GV-System 99
7.2.1 Defining ID Numbers for Multiple Camera Readers 99
7.2.2 Overlaying Card Numbers on Live View.....101

Chapter 8 CMS Configurations.....103
8.1 Center V2 103
8.2 VSM.....106
8.3 Dispatch Server 107

Chapter 9 Mobile Phone Connection 108
9.1 GV-Eye / GV-Eye HD for iPhone, iPod Touch and iPad.....108
9.1.1 Installing GV-Eye / GV-Eye HD.....109
9.1.2 Connecting to the Camera Reader.....109
9.2 GV-Eye for Android Smartphone and Tablet.....111
9.2.1 Installing GV-Eye for Android.....111
9.2.2 Connecting to Camera Reader 112
9.2.3 Accessing Live View 114

Specifications 115

Appendix 119

A. Settings for Internet Explore 8.....119

B. RTSP Protocol Support.....120

C. The CGI Command.....120

Naming and Definition

GV-System	GeoVision Analog and Digital Video Recording Software. The GV-System also refers to **Multicam System**, **GV-NVR System**, **GV-Hybrid DVR System** and **GV-DVR System** at the same time.

Chapter 1 Introduction

All-in-One Solution

GV-CR420 is a card reader with a built-in 4 MP wide angle IP camera. The card reader recognizes identification cards and grants access accordingly. The wide angle camera captures all angles of the entrance and transmits live view to GV-ASManager and GV-System through network connection. The all-in-one solution eliminates the need of installing and maintaining a separate camera in addition to the card reader.

Card and Face Mode

In addition to granting access after a card is presented, the integration of card reader and wide angle camera allows you to enable the Card and Face Mode, where the camera reader needs to be able to both recognize the card and detect a face before access is granted.

Web Interface

Using a browser, you can watch live view and utilize functions such as motion detection, privacy mask and alert notifications through the Web interface.

There are three ways to connect the camera reader to a GV-AS Controller: through **RS-485**, **Wiegand** or **Network** connection.

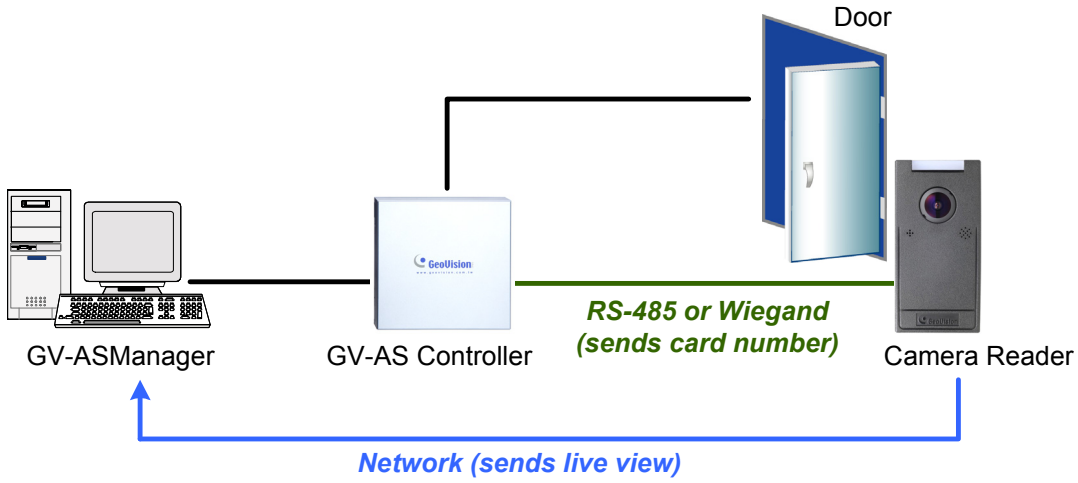


Figure 1-1 RS-485 or Wiegand Connection

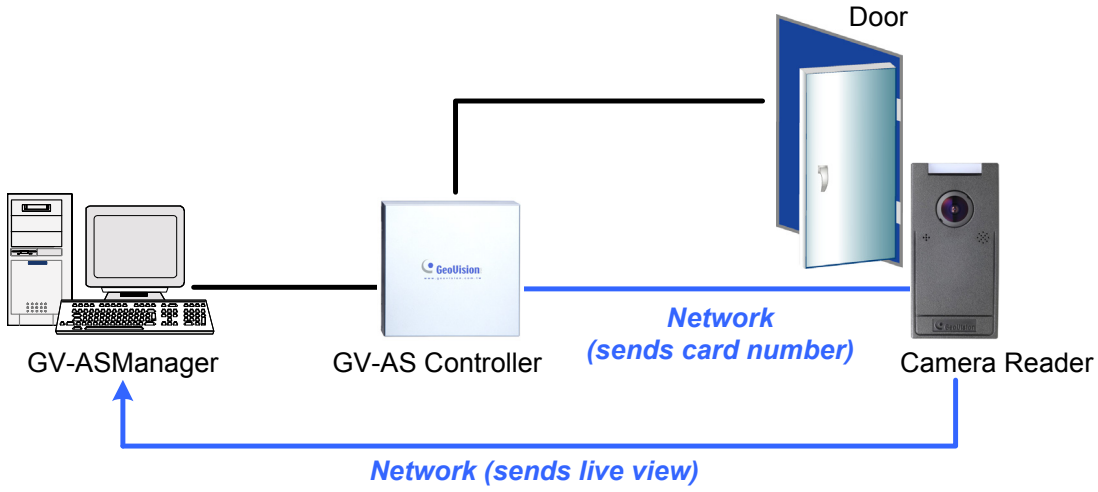


Figure 1-2 Network Connection

1.1 Key Features

Camera

- Wide angle IP camera with 4 MP progressive scan CMOS
- Stream 1 from H.264 and MJPEG
  Stream 2 from H.264 and MJPEG
- Up to 15 fps at 2048 x 1944
- Built-in Web server for monitoring through Internet Explorer web browser
- Built-in microphone and speaker
- Wide Dynamic Reader (WDR)
- Defog
- Privacy mask to cover parts of the image that should not be viewable
- Tampering alarm
- Text overlay
- 28 languages on web interface
- ONVIF conformant

Reader

- GV-AS Controller connection through Wiegand interface, RS-485 interface and network
- 13.56 MHz for ISO14443A (Mifare DESFire, Mifare Plus and Mifare Class)
- Access by card plus face detection

Access Control

- Enabling different access control modes according to the Authentication Schedule: Card only mode (default), Card and Face Mode
- Receiving live view and capturing snapshots when card is presented

1.2 Packing List

- GV-CR420 x 1

- Mounting Plate x 1

- Standard Screw x 2

- Plastic Screw Anchor x 2

- Security Screw x 1

- Torx Wrench x 1

- DC 12V Power Adapter x 1
- Software DVD x 1
- Quick Start Guide x 1

1.3 Optional Accessories

Name	Details
GV-AS ID Card and GV-AS ID Tag	• GV-AS ID Card and GV-AS ID Tag are fully compatible with GV-Camera Reader • 13.56MHz, Mifare

1.4 System Requirements

To operate the camera through a web browser, make sure your PC has good network connection, and use one of the following web browsers:

- Internet Explorer 7.x or later

Note: If you are using Microsoft Internet Explorer 8.0, additional settings are required. Refer to *Settings for Internet Explorer 8* in Appendix A.

Compatible GV-AS Controllers

- **GV-AS100 / 110 / 120 / ASBox / ASNet:** Firmware version 1.05 or later
- **GV-AS210:** Firmware version 1.1.0 or later
- **GV-AS400:** Firmware version 1.04 or later
- **GV-AS810:** Firmware version 1.1.0 or later

Note: Card and Face Mode by schedule and receiving card numbers through network connection are only supported in the following firmware versions.

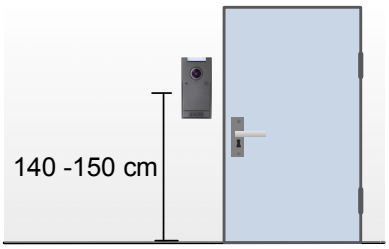
- **GV-AS100 / 110 / 120 / ASBox / ASNet:** Firmware version 1.06 or later
- **GV-AS210:** Firmware version 1.1.0 or later
- **GV-AS400:** Firmware version 1.04 or later
- **GV-AS810:** Firmware version 1.1.0 or later

1.5 Limitations and Optimal Installation for Face Detection

To make sure the face of the cardholder can be detected, follow the instructions below to install the camera reader.

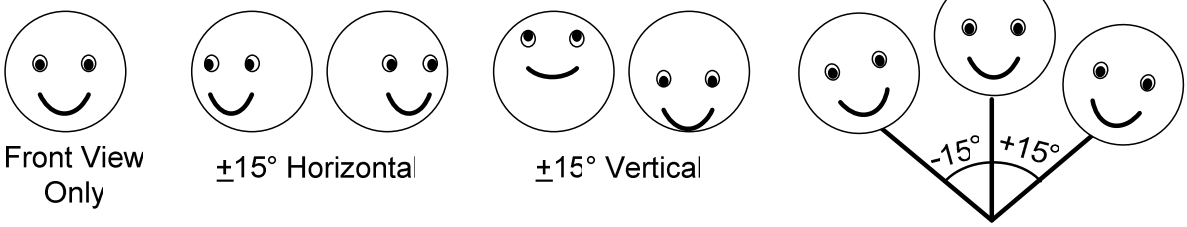
Installation Height:

- When placed at a building gate, the camera reader should be about 1.4-1.5 meters above the ground.
- When placed at a parking lot gate, the camera reader should be about 1.2 meters above the ground to match the height of vehicles.



Face Detection Limitations

- The camera reader cannot detect the face of cardholders wearing facial masks or sunglasses.
- The camera reader is designed to detect front-view faces only. If the face is slightly tilted horizontally or vertically, the tilt angle cannot exceed 15° degree.



Lighting Conditions

- The lighting of the entrance should be sufficient with minimum illumination no less than 41-50 Lux.
- Avoid placing the camera reader where the light source is directly behind the subject.

1.6 Physical Description

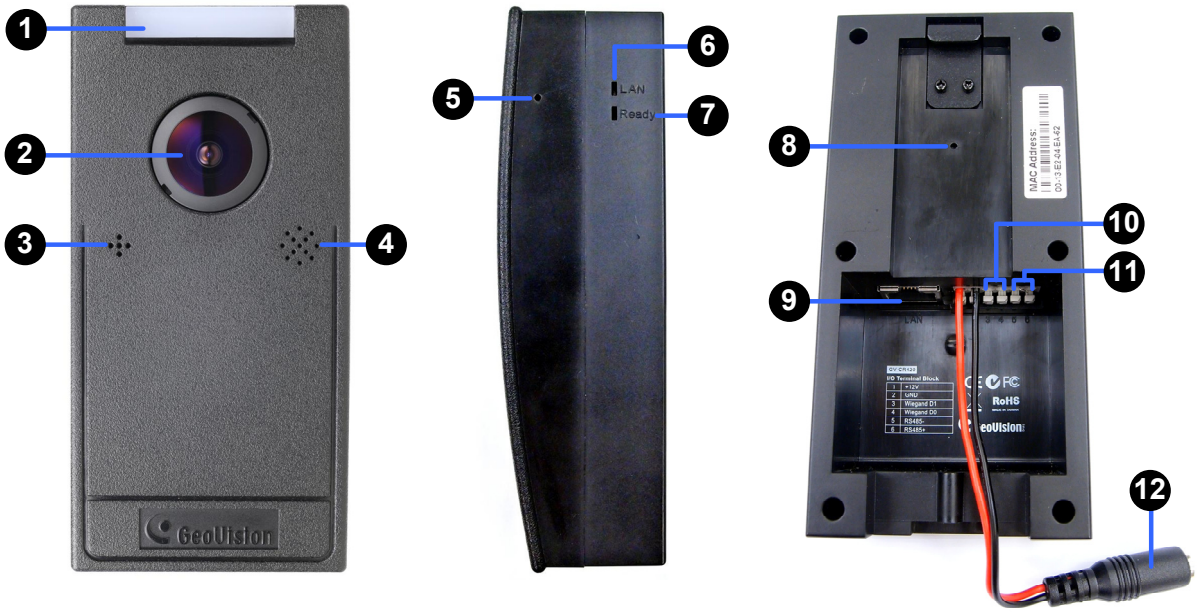
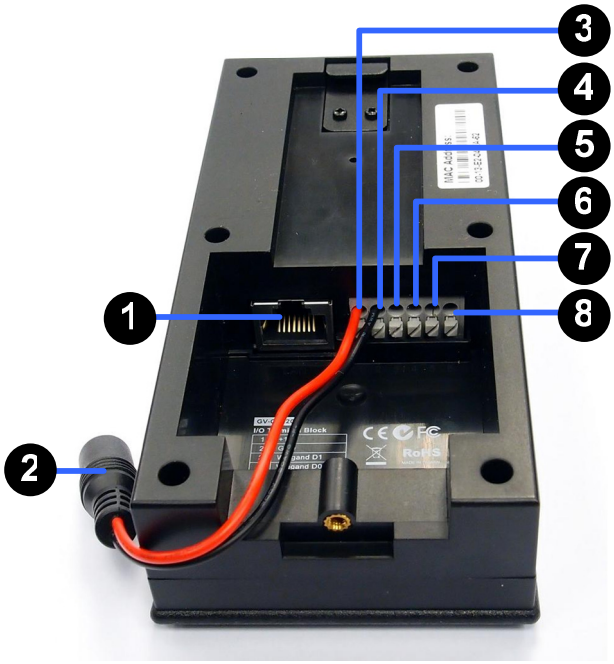


Figure 1-3

No.	Name	Function
1	LED Indicator	Shows the status of the reader. Blue LED indicates ready; green LED means card swiped; red LED indicates no face detected when Card and Face Mode is enabled.
2	Lens	Receives image.
3	Microphone	Receives the sound from the camera.
4	Speaker	Talks to the surveillance area from the local computer.
5	Beeper	Generates sound to signal reader status.
6	Network status LED	Indicates the network status.
7	Ready status LED	Indicates whether the unit is ready for use.
8	Default Button	Resets all configurations to default factory settings. See *6.3 Restoring to Factory Default Settings*.
9	Ethernet Port	Connects to network and allows network connection with GV-AS Controller.
10	Wiegand	Connects to a GV-AS Controller through Wiegand connection.
11	RS-485	Connects to a GV-AS Controller through RS-485 connection.
12	Power Cable	Connects to power supply.

1.7 Connecting the Cables and Wires

On the back of the camera reader, you will find an Ethernet port, a power connector and pins for Wiegand and RS-485 connection. The Wiegand and RS-485 interface allows you to connect the camera reader to a GV-AS Controller.



No.	Function
1	Ethernet
2	Power Cable
3	+12V
4	GND
5	Wiegand D1
6	Wiegand D0
7	RS485-
8	RS485+

Figure 1-4

1. Connect to network using the Ethernet port.
2. Connect the power cable to the supplied power adaptor.
3. To connect to GV-AS Controller through Wiegand interface,
   a. Insert a wire into the Wiegand D1 pin on the terminal block and press the screw below the pin with a small flat-tip screwdriver to secure it. Repeat with Wiegand D0.
   b. Connect the other end of the wire to the Wiegand interface of the controller.
   c. Connect a wire to the GND pin of the camera reader in addition to the existing black GND wire for power cable, and connect the other end to the GND of the Wiegand interface.
4. To connect to GV-AS Controller through RS-485 interface,
   a. Insert a wire into the RS485- pin on the terminal block and press the screw below the pin with a small flat-tip screwdriver to secure it. Repeat with RS485+.
   b. Connect the other end of the wire to the RS-485 interface of the controller.

1.8 Installation

After the location of the camera reader is decided, follow the steps below to install the camera reader.

1. Place the mounting plate on the wall with the oval-shaped hole toward the top.

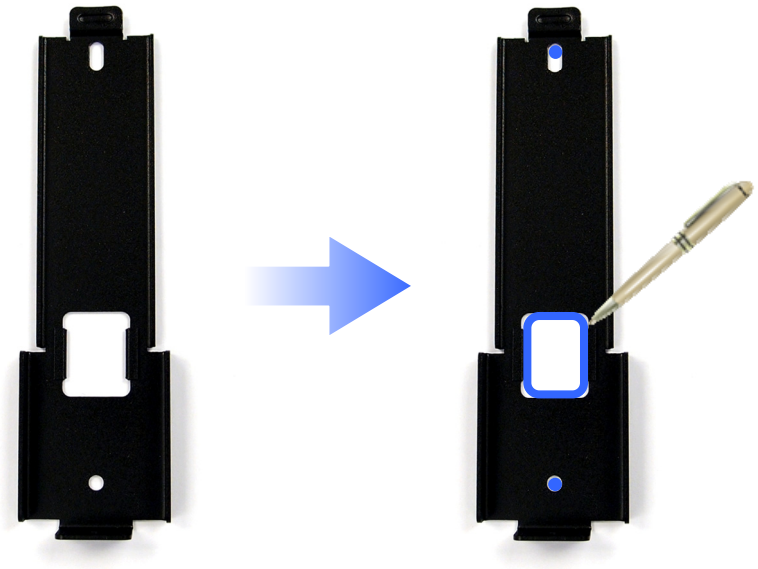


Figure 1-5

2. Mark the location of the 2 holes and the rectangle as labeled above.
3. Drill the rectangle to create a space for running the cables and wires.
4. At the 2 dots, drill a hole slightly smaller than the plastic screw anchors provided.
5. Insert the 2 plastic screw anchors in the drilled holes.
6. Place the mounting plate on the wall and secure with the 2 standard screws provided.

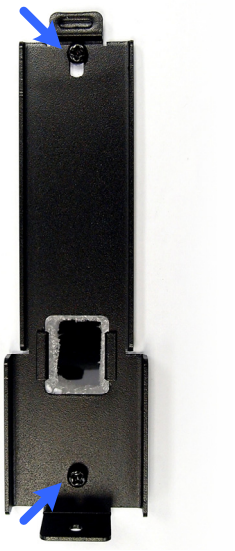


Figure 1-6

7. Place camera reader on the mounting plate and thread the cables through the rectangular hole.

Figure 1-7

8. Secure the security screw on the bottom.

Figure 1-8

Chapter 2 Access Control Configurations

This chapter explains how to set up access control related functions by integrating GV-CR420 with GV-AS Controller and GV-ASManager.

1. Connecting GV-CR420 to GV-AS Controller

This section explains how to connect GV-CR420 to GV-AS Controller and define the associated door.

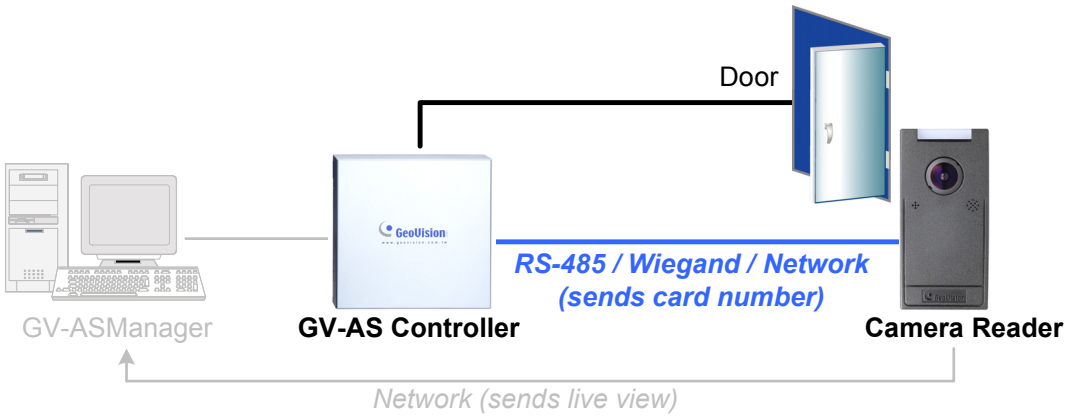


Figure 2-1

2. Setting up GV-ASManager

This section explains how to add GV-AS Controller to GV-ASManager, set up schedule, and receive GV-CR420 live view on GV-ASManager.

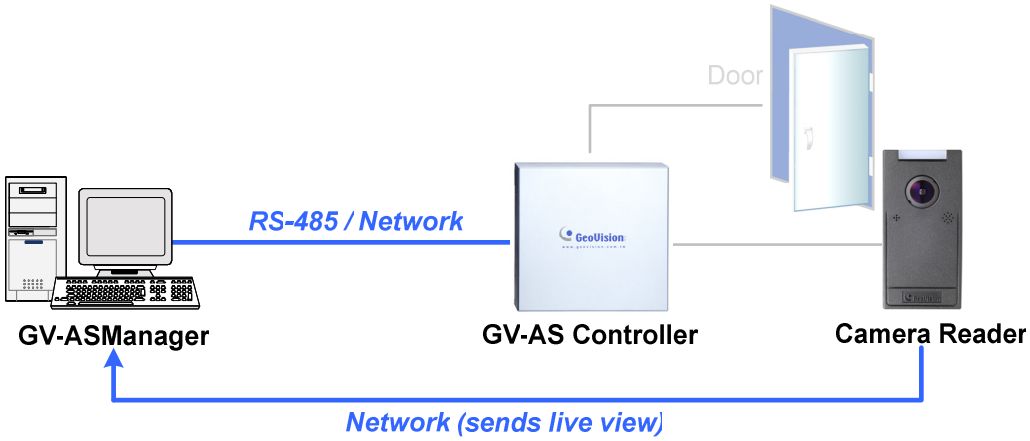


Figure 2-2

2.1 Connecting to GV-AS Controller

There are three ways to connect a camera reader to GV-AS Controllers: **Wiegand**, **RS-485** and **network**. Below is a list of the type of connections and the number of GV-CR420 supported by different GV-AS Controller models.

GV-AS Controller Model	Number of Camera Readers Supported	
	Wiegand	RS-485 / Network
GV-AS100	1	1
GV-AS110 / 120	1	Not supported
GV-AS100 / 110 / 120 with GV-ASBox	2	4
GV-AS100 / 110 / 120 with GV-ASNet	Not supported	2
GV-AS210	4	8
GV-AS400	8	8
GV-AS810	8	8

2.1.1 Through Wiegand Interface

1. Wire GV-CR420 to GV-AS Controller

a. Connect a wire to the Wiegand pins of the GV-CR420 and the other end to the Wiegand interface on the controller.

b. Connect a wire to the GND pin of the camera reader in addition to the existing black GND wire for power cable and connect the other end to the GND of the Wiegand interface.

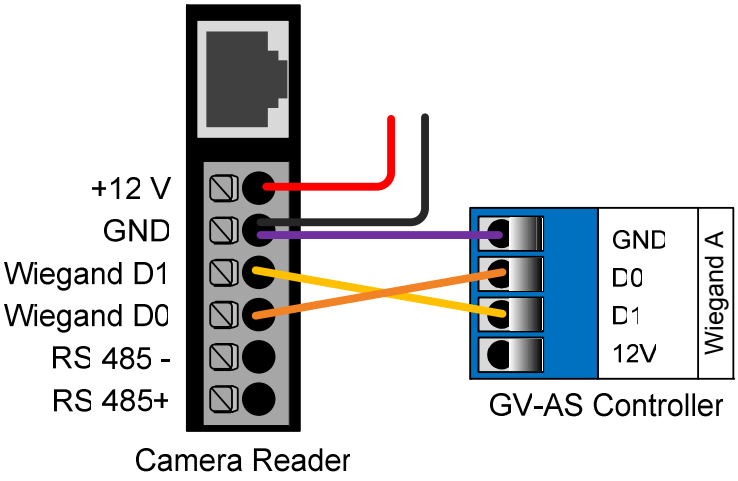


Figure 2-3

For detailed instructions, refer to *1.7 Connecting the Cables and Wires* earlier in this manual and the *Connecting a Wigand Reader* or *Connecting Card Readers* section in the *GV-AS Controller User's Manual*.

Note: Each camera reader must be connected to a power adaptor instead of using the power from GV-AS Controller.

---

2. Define the door associated with GV-CR420 on the GV-AS Controller

a. Access the Web interface of the GV-AS Controller.
For detailed instructions, refer to the *Web-Based Configurations* section in the *GV-AS Controller User's Manual*.

b. In the left menu, click **Wiegand Setting** or **Function Setting** depending on the type of controller.

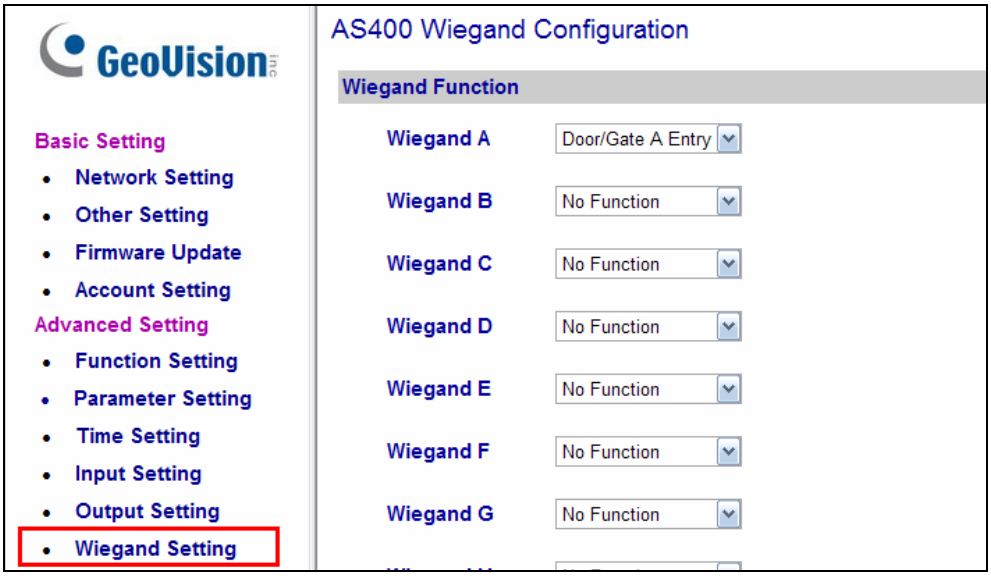


Figure 2-4

c. Use the drop-down list to select the associated door.

d. Click **Submit** to apply the settings.

2.1.2 Through RS-485 Interface

1. Wire GV-CR420 to GV-AS Controller

Connect a wire to the RS-485 pins of the GV-CR420 and the other end to the RS-485 interface on the controller.

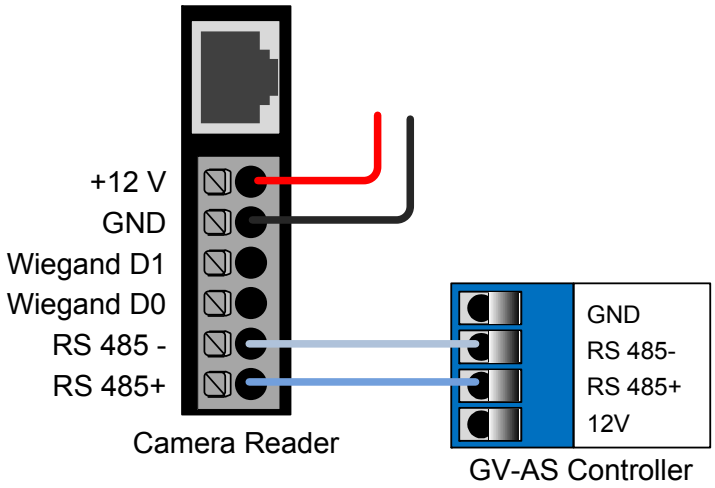


Figure 2-5

For detailed instructions, refer to *1.7 Connecting the Cables and Wires* earlier in this manual and the *Connecting a Wigand Reader* or *Connecting Card Readers* section in the *GV-AS Controller User's Manual*.

Note: Each camera reader must be connected to a power adaptor instead of using the power from GV-AS Controller.

---

2. Define the door associated with GV-CR420 on the GV-AS Controller

a. Access the Web interface of the GV-AS Controller.
For detailed instructions, refer to the *Web-Based Configurations* section in the *GV-AS Controller User's Manual*.

b. In the left menu, click **Extended Reader**.

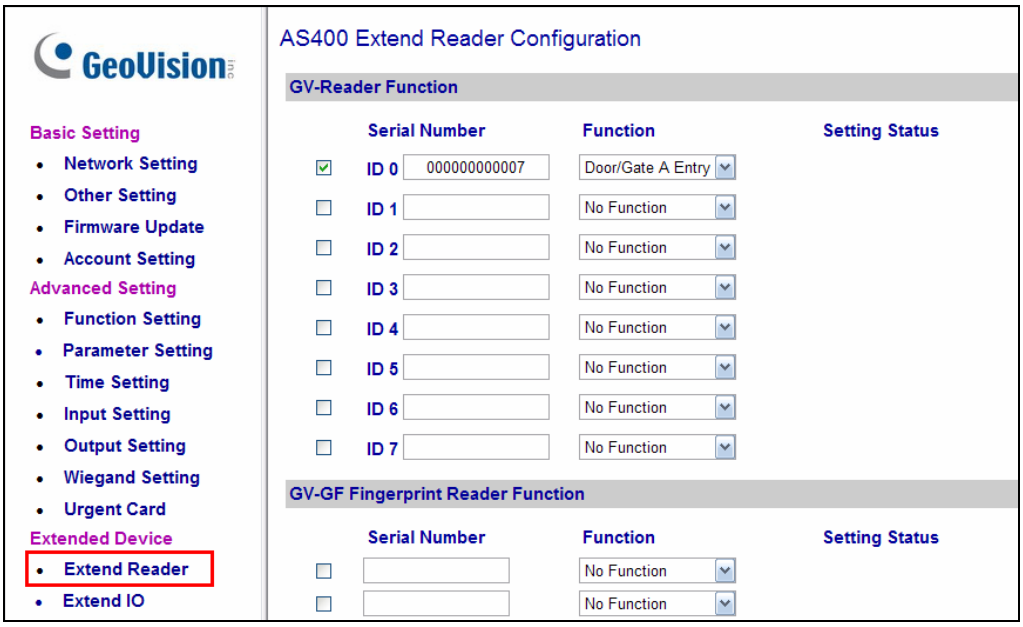


Figure 2-6

c. Select an ID, type the barcode of the camera reader, and use the drop-down list to select the associated door.

d. Click **Submit** and the Setting Status should turn green.

2.1.3 Through Network Connection

Each GV-CR420 can only be connected to one AS Controller at a time.

1. **Enable network connection to AS Controller on GV-CR420**

   a. Access the Web interface of the GV-CR420. Refer to Chapter 3, *Establishing Network Connection*.

   b. In the left menu, click **Video Settings** and select **Streaming 1**.

   c. Under Face Detection Setting, select **Enable network connection to AS Controller** and use the drop-down list to select the controller.

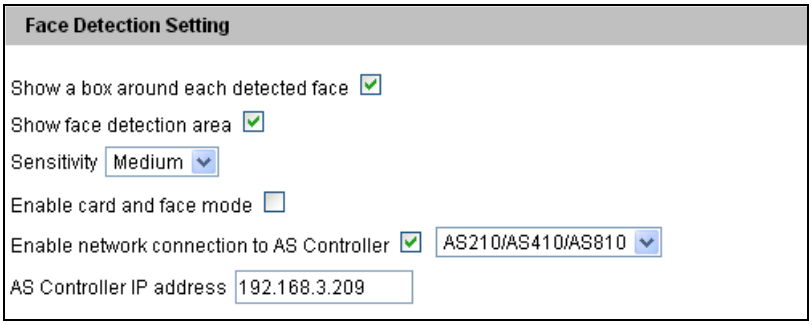


Figure 2-7

   d. Type the IP address of the GV-AS Controller.

   e. Click **Apply**.

Note: The LED Indicator of GV-CR420 will be a constant pink light if network connection with the Controller is interrupted. This function is only supported by GV-AS210 / 810 firmware version 1.1.0 or later.

---

2. **Define the door associated with GV-CR420 on the GV-AS Controller**

   a. Access the Web interface of the GV-AS Controller.
   For detailed instructions, refer to the *Web-Based Configurations* section in the *GV-AS Controller User's Manual*.

   b. In the left menu, click **Extended Reader** under the Extended Device section.

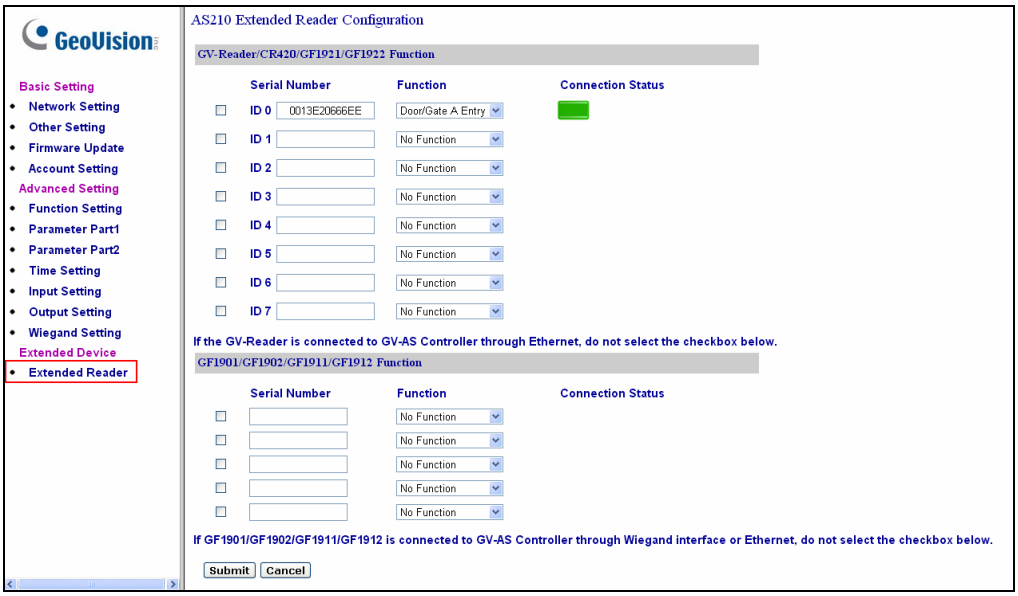


Figure 2-8

   c. Select an ID, type the barcode / MAC address of the camera reader according to the firmware version of GV-CR420 and the controller, and use the drop-down list to select the associated door. For details on firmware version and corresponding methods of network connection, see the note below.

   d. Click **Submit** and the Setting Status should turn green.

Note:

1. Network connection between GV-CR420 firmware V1.0.1 and GV-AS210 / 810 firmware V1.1.0 can only be established using **MAC address**. Network connection between GV-CR420 firmware V1.0 and GV-AS210 / 810 firmware V1.0 can only be established using **barcode**.
2. Network connection between GV-CR420 and GV-AS400 or GV-AS100 / 110 / 120 through ASBox / ASNet is only supported using barcode.

2.2 Setting Up GV-ASManager

Integration with GV-ASManager allows you to utilize full access control functions. This section covers basic settings on how to add GV-AS Controller to GV-ASManager, set up an access control schedule, and receive live view from GV-CR420 on GV-ASManager.

For more details on GV-ASManager functions, refer to the *GV-ASManager User's Manual*.

2.2.1 Adding GV-AS Controller

1. On the menu bar of GV-ASManager, click **Setup** and select **Device**. The Controller List dialog box appears
2. Click the **Add** icon on the top left corner. This dialog box appears.

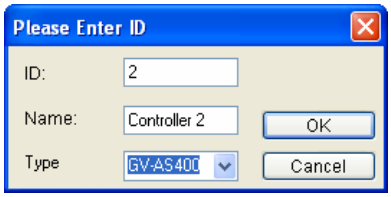


Figure 2-9

3. Enter **ID** and **Name** of the Controller, select the **Type** of the Controller and click **OK**. This dialog box appears.

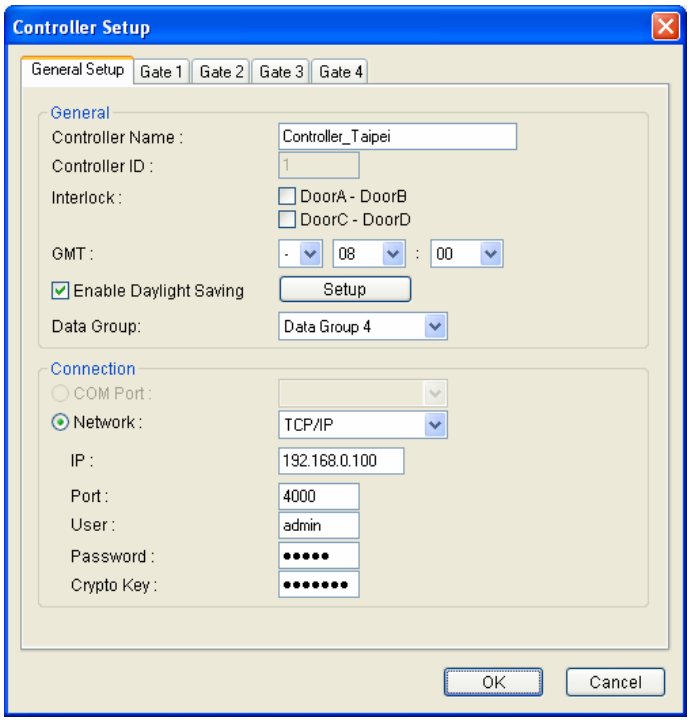


Figure 2-10

Note: The Controller ID is set ahead with GV-ASKeypad or Web interface. Refer to *GV-AS Controller User's Manual* for details.

4. In Connection section, select the communication mode between the GV-AS Controller and GV-ASManager.
   - For RS-485 connection, select **COM Port** that is used for connection.
   - For network connection, select **Network** and select **TCP/IP** or **LocalDDNS**. Type the IP address, device name (if LocalDDNS is selected), port number, login user, login password and Crypto key (3DES code) of the GV-AS Controller.

Note: The default values of GV-AS Controller are: IP address **192.168.0.100**; username **admin**; password **admin**; Crypto key (3DES code) **12345678**.

5. To check if the above connection settings are correct, you can click **OK** at this step and back to the main screen. The icon appearing on the Device View window indicates the connection is established.

2.2.2 Setting Up Access Control Schedule

Follow the steps below to set a schedule with different access modes:

1. Click the **Door/Gate** tab in the Controller Setup dialog box.

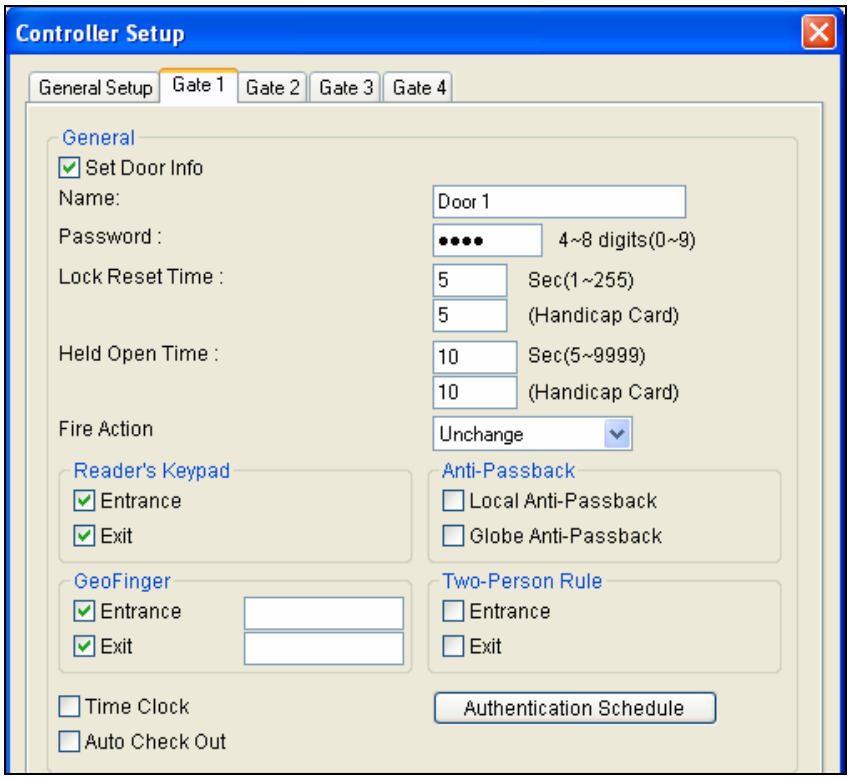


Figure 2-11

2. In the General section, enable **Set Door Info** to define the general parameters for the door. The default password is **admin**.

3. To set a schedule to specify different access modes at different periods of time, click the **Authentication Schedule** button.

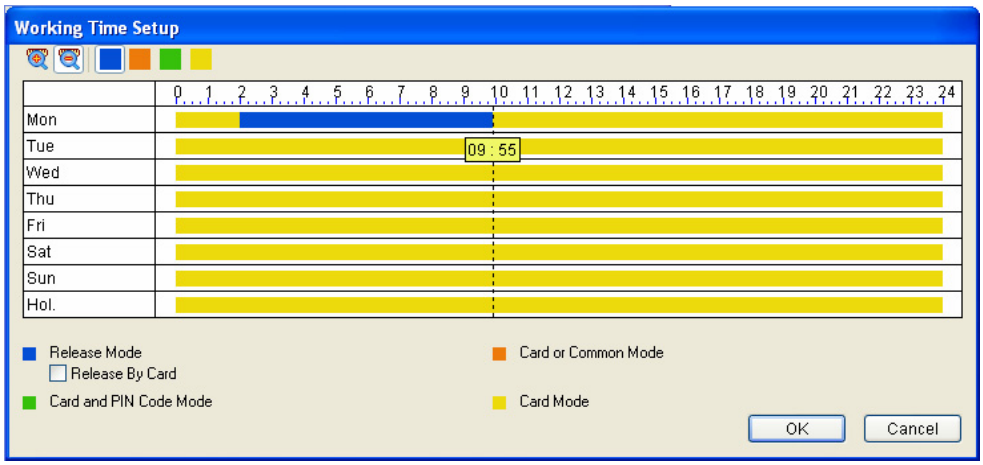


Figure 2-12

4. To define which kind of access mode should be applied at specific day and time, select one access mode on the toolbar and drag the mouse over the timelines.

   - **Card Mode:** This is the default mode. This mode only requires the user to present his or her card to be granted access.
   - **Release Mode:** Keep the door in an unlock status with the reader.
     - **Release by Card:** The door will unlock only after a card is presented and will remain unlocked during the time specified for Release Mode. This option is designed to prevent unattended doors from opening during the Release Mode time.
   - **Card and PIN Code Mode:** For GV-CR420, a card needs to be presented and GV-CR420 needs to be able to detect a face before access is granted. For other readers, a card and the correct pin code is required to gain access.
   - **Card or Common Mode:** For GV-CR420, this mode is the same as the Card Mode. For readers with keypad, users can choose to present a card or enter the door's password to be granted access.

Tip: You can apply Card Mode during business hours and apply Card and PIN Code Mode at night when higher security is necessary.

5. Click **OK** several times and return to the main screen. If the icon appears, it indicates the connection between the controller and GV-ASManager has been established.

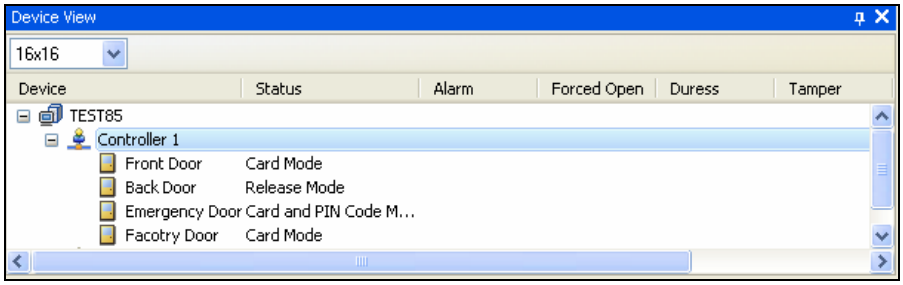


Figure 2-13

2.2.3 Receiving Live View from Camera Reader

To receive live view of the camera reader on the GV-ASManager, follow the steps below.

Note: To receive live view and take snapshots of the camera reader, you must connect it to the network in advance. See *Chapter 3 Establishing Network Connection*.

---

1. Click the **Door/Gate** tab in the Controller Setup dialog box.

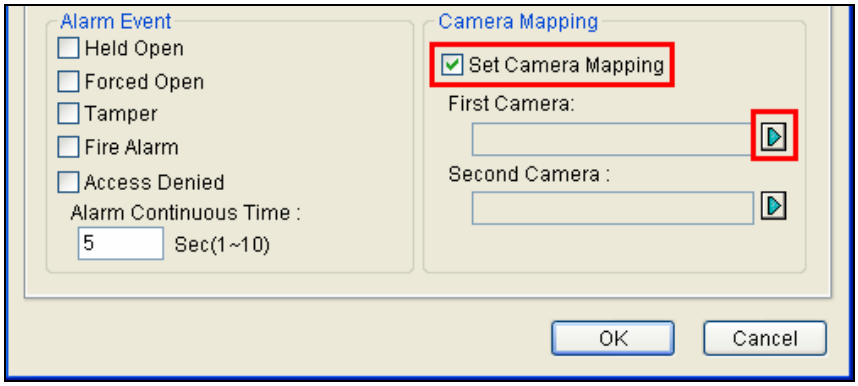


Figure 2-14

2. In the Camera Mapping section, select **Set Camera Mapping** and click the first **Arrow** button. This dialog box appears.

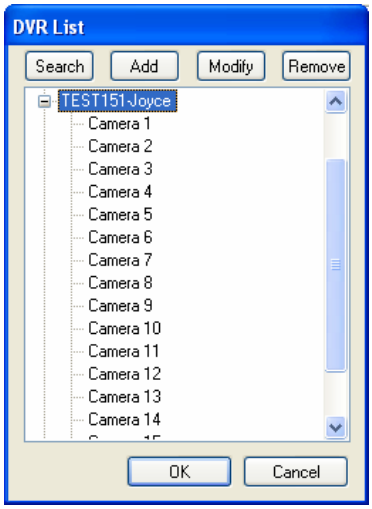


Figure 2-15

3. To connect the camera reader to the GV-ASManager, use one of these ways:
   - Click **Add**, select the type of the IP device, and enter its IP address and login information.
   - Click **Search** to detect all GeoVision IP devices on the same LAN. After adding the camera reader, you must click the **Modify** button to enter its login ID and password.

Note: For GV-ASManager 3.0 or before, select GV-FE420 for the device type and for GV-ASManager 4.0 or later, select GV-CR420 for the device type.

4. Expand the Host folder listed in the DVR List dialog box (*Figure 5-2*), select a camera reader and click **OK**. The mapped **Host Name** and **Camera** are displayed on the Controller Setup dialog box.
5. To map the second camera reader to the door, click the second **Arrow** button, and follow Steps 3 and 4 to add another camera.
6. Click **OK** and return to the main screen.
7. Click the specific door on the Device View window.

The associated live view is displayed on the Live Video window. When a compatible but not enrolled card is swiped, you can right-click the “Access Denied: Invalid Card” message and select **New/Edit Card** to enroll the card. For details on enrolling cards, refer to the *Setting Cards* section in the *GV-ASManager User’s Manual*.

You can also click the **Tiles** or **Thumbnails** tab in the Access Monitor Window to see snapshots from the camera reader captured whenever a card is presented.

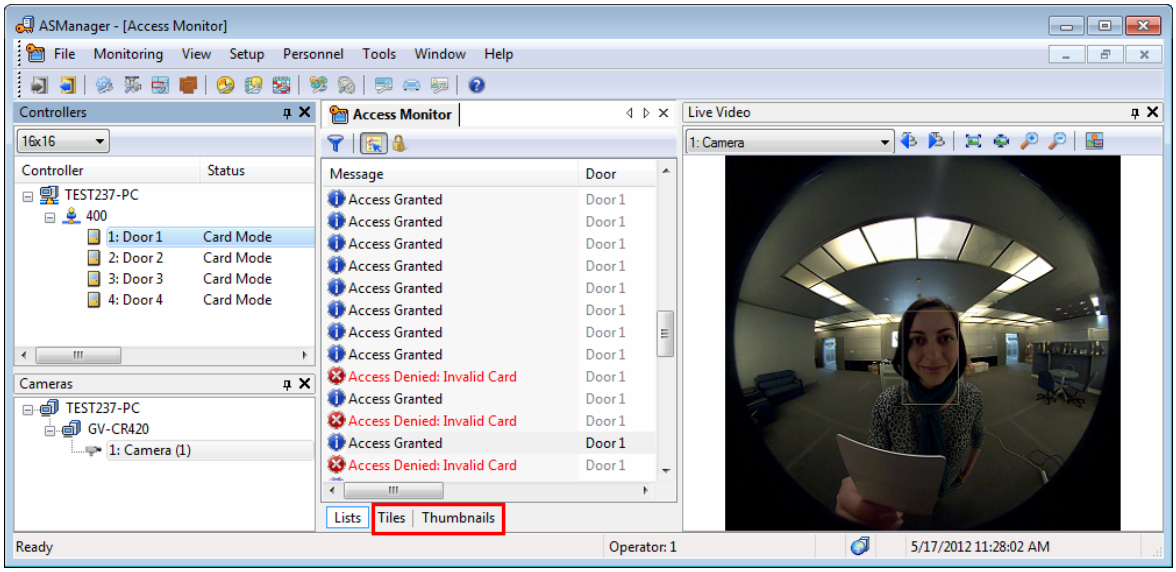


Figure 2-16

Chapter 3 Establishing Network Connection

Follow the steps below to get the camera reader working on the network:

1. Using a standard network cable, connect the camera to your network.
2. Using the supplied power adapter, connect to power.
3. You can now access the Web interface of the camera reader.
    - If the camera reader is installed in a LAN with the DHCP server, use GV-IP Device Utility to look up the camera reader's dynamic IP address. See *3.1 Checking the Dynamic IP Address*.
    - If the camera reader is installed in a LAN without the DHCP server, the default IP address 192.168.0.10 will be applied. You also can assign a different static IP address. See *3.2 Assigning an IP Address*.

Note: By default, the camera reader has the IP address **192.168.0.10**, and ID and password **admin**.

Once the camera reader is properly installed, the following important features can be configured using the browser-based configuration page and are discussed in the following sections in this manual:

- **Date and time adjustment:** see *5.5.1 Date and Time Settings*.
- **Login and privileged passwords:** see *5.5.3 User Account*.
- **Network gateway:** see *5.4 Network*.
- **Camera image adjustment:** see *4.2.2 The Control Panel of the Live View Window*.
- **Video format, resolution and frame rate:** see *5.1.1 Video Settings*.

3.1 Checking the Dynamic IP Address

Follow the steps below to look up the IP address and access the Web interface.

Note: The PC installed with GV-IP Device Utility must be under the same LAN with the camera reader you wish to configure.

1. Install the GV-IP Device Utility program included on the Software DVD.
2. On the GV-IP Utility window, click the button to search for the IP devices connected in the same LAN. Click the **Name** or **Mac Address** column to sort.

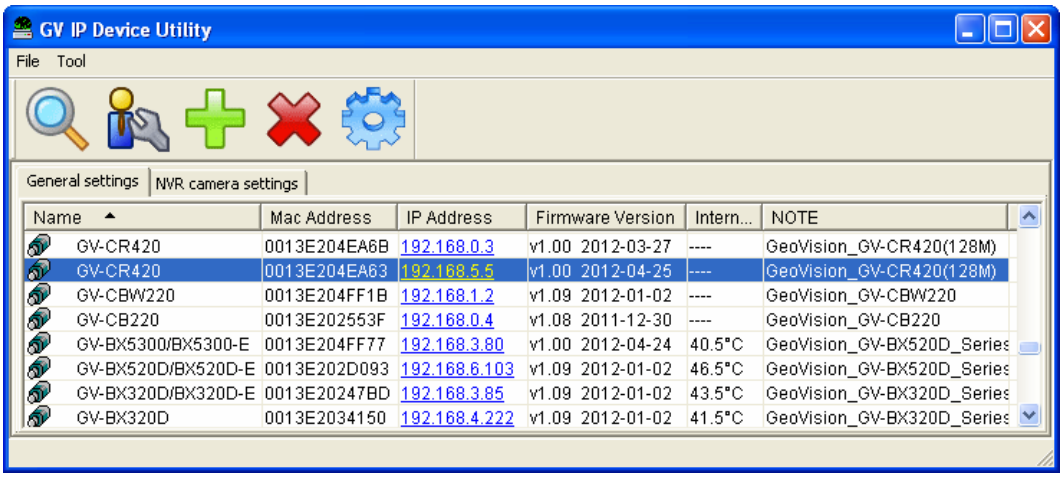

GV IP Device Utility
File Tool
General settings
NVR camera settings
Name
Mac Address
IP Address
Firmware Version
Intern...
NOTE
GV-CR420 0013E204EA6B 192.168.0.3 v1.00 2012-03-27 ---- GeoVision_GV-CR420(128M)
GV-CR420 0013E204EA63 192.168.5.5 v1.00 2012-04-25 ---- GeoVision_GV-CR420(128M)
GV-CBW220 0013E204FF1B 192.168.1.2 v1.09 2012-01-02 ---- GeoVision_GV-CBW220
GV-CB220 0013E202553F 192.168.0.4 v1.08 2011-12-30 ---- GeoVision_GV-CB220
GV-BX5300/BX5300-E 0013E204FF77 192.168.3.80 v1.00 2012-04-24 40.5°C GeoVision_GV-BX520D_Series
GV-BX520D/BX520D-E 0013E202D093 192.168.6.103 v1.09 2012-01-02 46.5°C GeoVision_GV-BX520D_Series
GV-BX320D/BX320D-E 0013E20247BD 192.168.3.85 v1.09 2012-01-02 43.5°C GeoVision_GV-BX320D_Series
GV-BX320D 0013E2034150 192.168.4.222 v1.09 2012-01-02 41.5°C GeoVision_GV-BX320D_Series

Figure 3-1

3. Find the camera reader with its MAC address, click on its IP address and select **Web Page**.

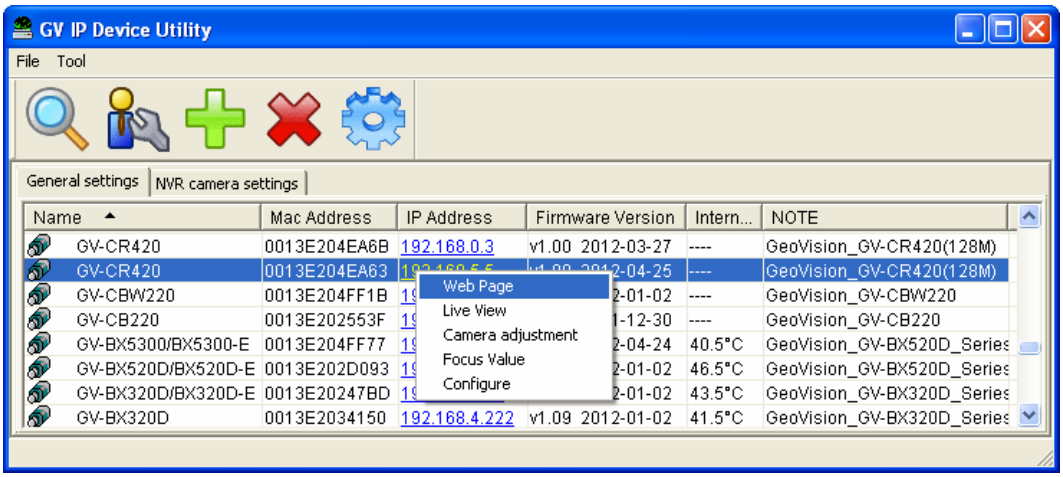


Figure 3-2

4. The login page appears.

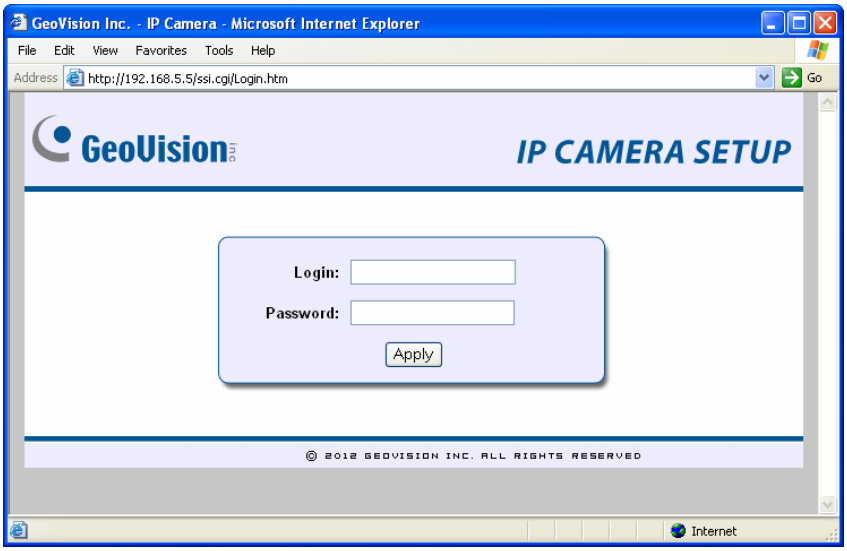


Figure 3-3

5. Type the default ID and password **admin** and click **Apply** to login.

3.2 Assigning an IP Address

Follow the steps below to assign a new IP address.

Note:

1. The camera reader has a default IP address of **192.168.0.10**. The computer used to set the IP address must be under the same network assigned to the unit.
2. If your router supports the DHCP server, the camera reader will obtain a dynamic IP address from the DHCP server each time it connects to the LAN, instead of using 192.168.0.10.

1. Open your web browser, and type the default IP address http://192.168.0.10
2. In both Login and Password fields, type the default value **admin**. Click **Apply**.
3. In the left menu, select **Network** and then **LAN** to begin the network settings.

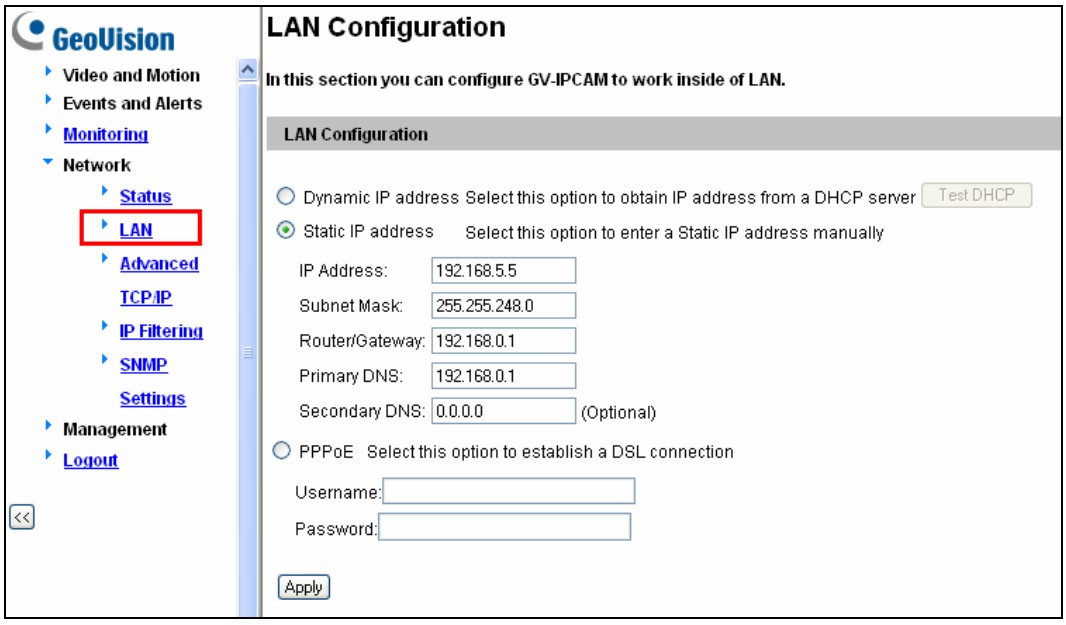


Figure 3-4

4. Select **Static IP address**. Type the IP Address, Subnet Mask, Router/Gateway, Primary DNS and Secondary DNS.
5. Click **Apply**. The camera reader is now accessible by entering the assigned IP address on the web browser.

IMPORTANT:

- If **Dynamic IP Address** or **PPPoE** is enabled, you need to know which IP address the camera reader will get from the DHCP server or ISP to log in. If your camera reader in installed in a LAN, use the GV-IP Device Utility to look up its current dynamic address. See *3.1 Checking the Dynamic IP Address*.
  If your camera reader uses a public dynamic IP address, via PPPoE, use the Dynamic DNS service to obtain a domain name linked to the camera reader's changing IP address first. For details on Dynamic DNS Server settings, see *5.4.2 Advanced TCP/IP.*
- If **Dynamic IP Address** and **PPPoE** is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the network settings again.
  To restore the factory settings, see *6.3 Restoring to Factory Default Settings*.

Chapter 4 Accessing the Camera Reader

Two types of users are allowed to log in to the camera: **Administrator** and **Guest**. The Administrator has unrestricted access to all system configurations, while the Guest has the access to live view and network status only.

4.1 Accessing Your Surveillance Images

Once installed, your camera is accessible on a network. Follow these steps to access your surveillance images:

1. Start the Internet Explorer browser.
2. Type the IP address or domain name of the camera in the **Location / Address** field of your browser.

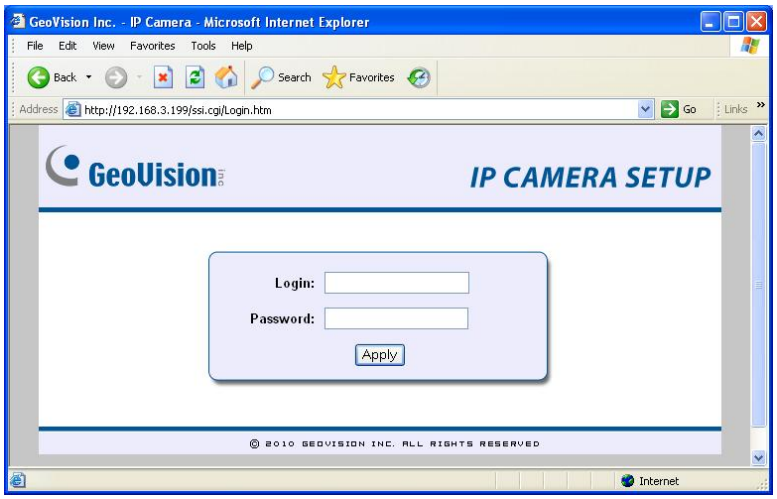


Figure 4-1

3. Enter the login name and password.
   - The default login name and password for Administrator are **admin**.
   - The default login name and password for Guest are **guest**.
4. A video image, similar to the example in Figure 4-2, is now displayed in your browser.

Note: To enable the updating of images in Microsoft Internet Explorer, you must set your browser to allow ActiveX Controls and perform a one-time installation of GeoVision's ActiveX component onto your computer.

4.2 Functions Featured on the Main Page

This section introduces the features of the **Live View** window and **Network Status** on the main page. The two features are accessible by both Administrator and Guest.

Main Page of Guest Mode

▼ **Video and Motion**
- ▼ **Live View**
  - ▶ Camera
- ▼ **Network**
  - ▶ Status

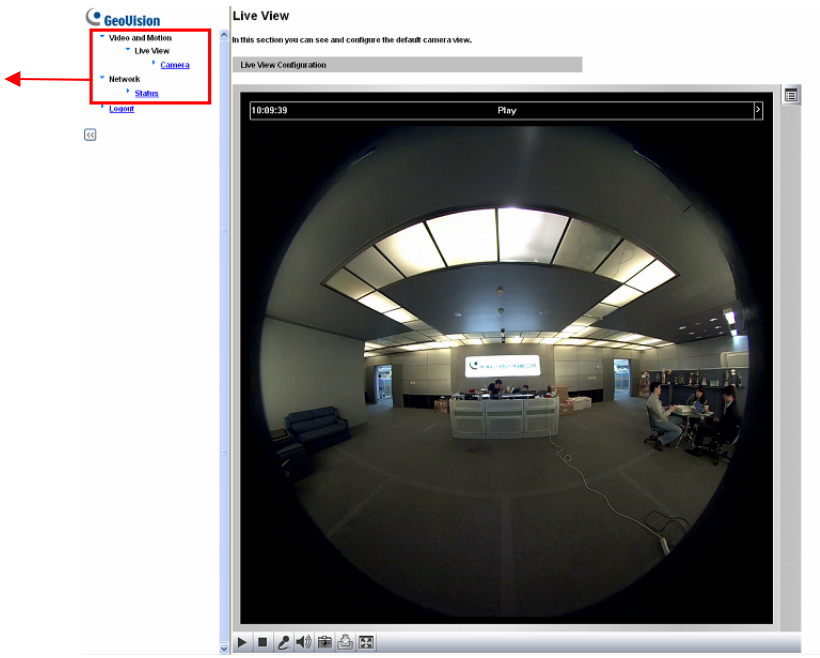


Figure 4-2

4.2.1 The Live View Window

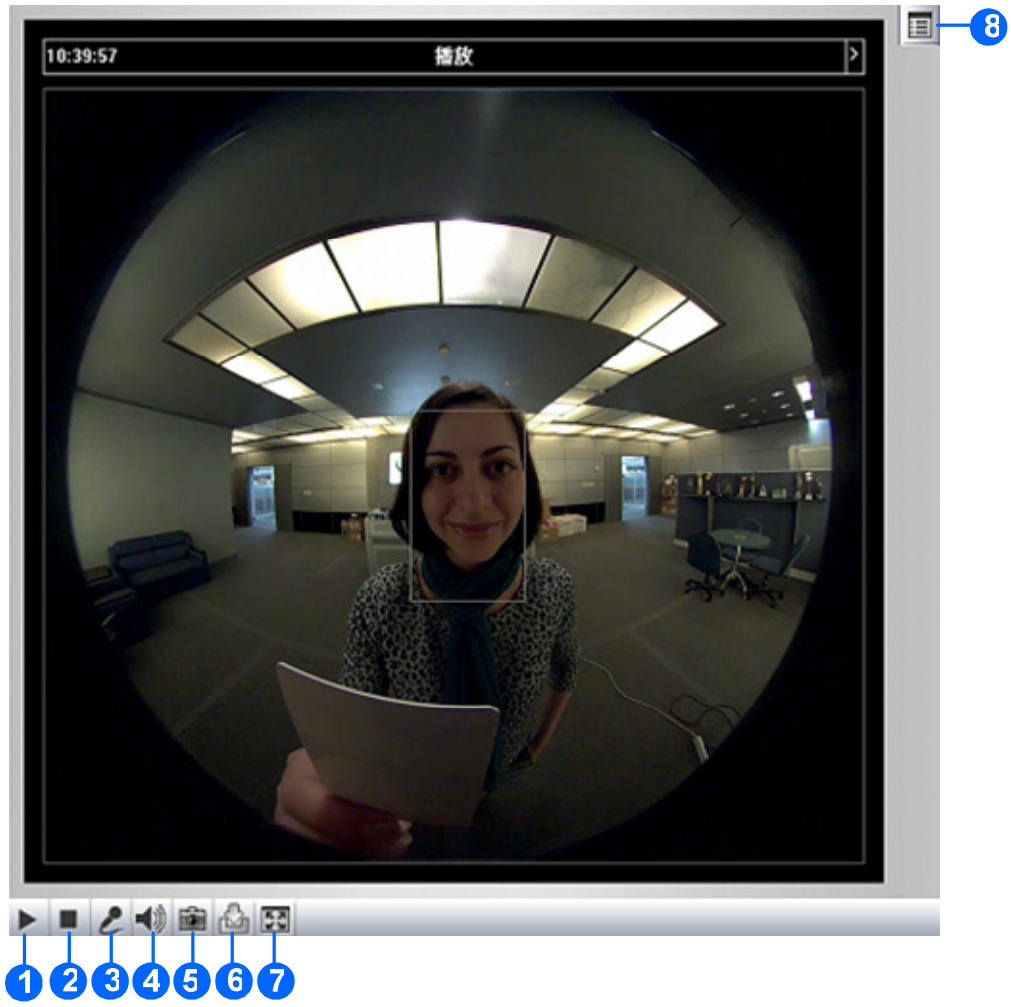


Figure 4-3

No.	Name	Function
1	Play	Plays live video.
2	Stop	Stops playing video.
3	Microphone	Talks to the surveillance area from the local computer.
4	Speaker	Listens to the audio around the camera.
5	Snapshot	Takes a snapshot of live video. --- See *4.2.3 Snapshot of a Live Video*.
6	File Save	Records live video to the local computer. --- See *4.2.4 Video Recording*.
7	Full Screen	Switches to full screen view. Right-click the image to have these options: **Snapshot**, **Resolution**, **PIP**, **PAP**, **GPS** and **Google Maps**. --- See *4.2.5 Picture-in-Picture and Picture-and-Picture View* --- See *5.5.2 GPS Maps Settings*

8	Show System Menu	Brings up these functions: **Alarm Notify**, **Video and Audio Configuration**, **Remote Config**, **Show Camera Name** and **Image Enhance**. --- See *4.2.6 Alarm Notification*, *4.2.7 Video and Audio Configuration*, *4.2.8 Remote Configuration*, *4.2.9 Camera Name Display* and *4.2.10 Image Enhancement* respectively.

4.2.2 The Control Panel of the Live View Window

To open the control panel of the Live View window, click the arrow button on top of the viewer. You can access the following functions by using the left and right arrow buttons on the control panel.

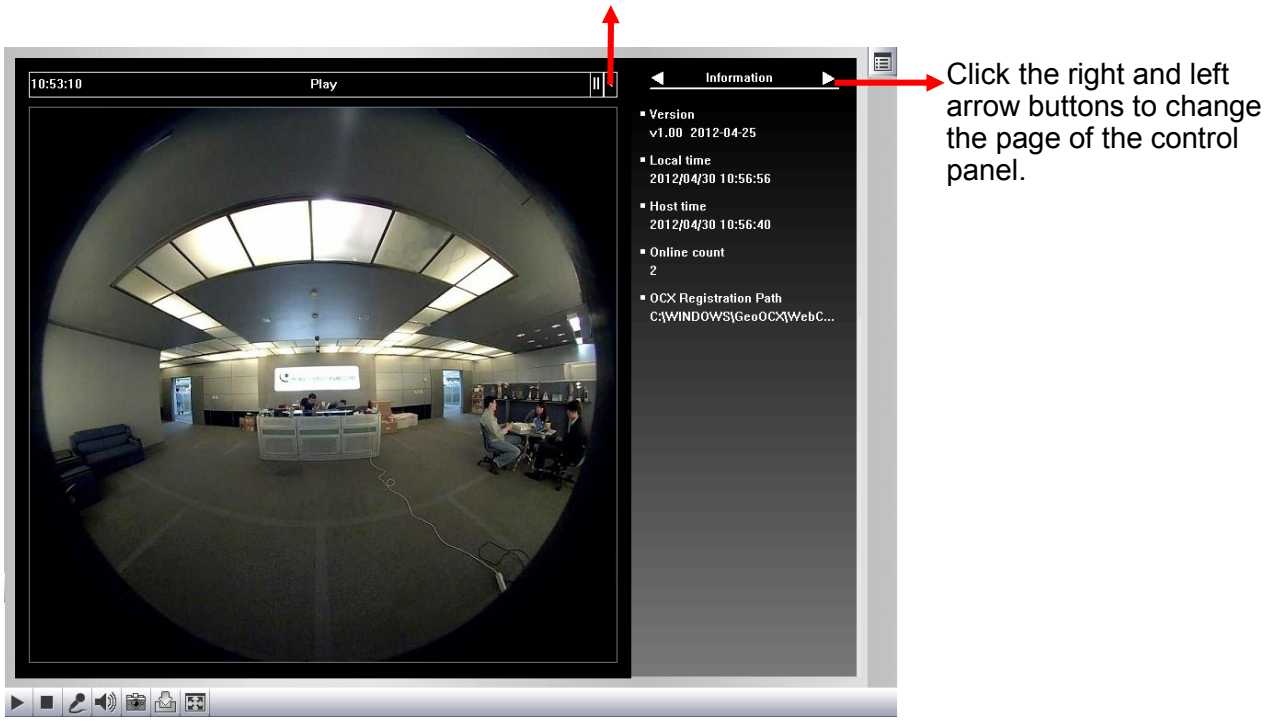


Figure 4-4

Tip: The administrator can also use the GV-IP Device Utility and click the camera's IP address to access the live view and adjust camera image settings.

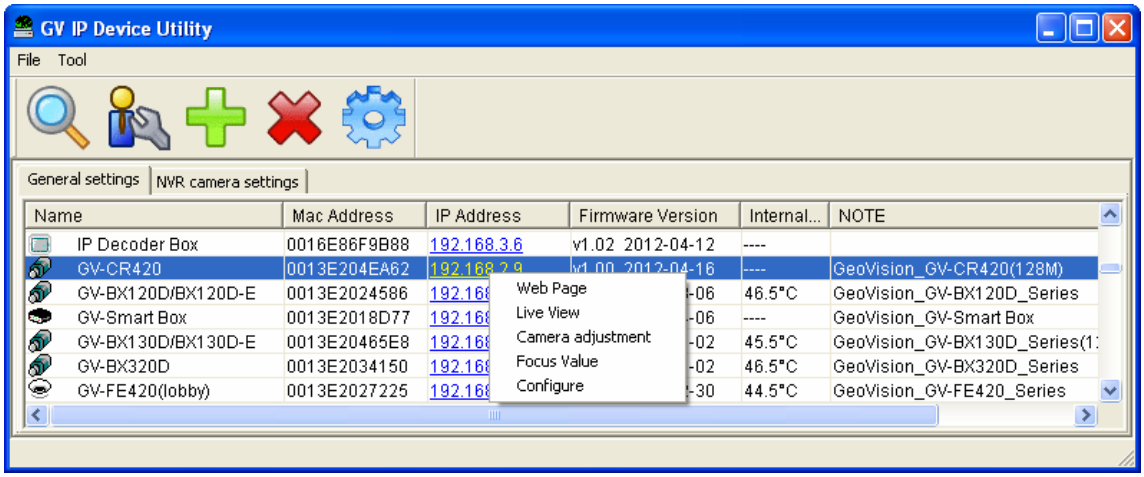


Figure 4-5

[Information] Displays the version of the camera, local time of the local computer, host time of the camera, and the number of users logging in to the camera.

[Video] Displays the current video codec, resolution and data.

[Audio] Displays the audio data rates when the microphone and speaker devices are enabled.

[Alarm Notify] Displays the captured images upon motion detection. For this function to work, you must configure the Alarm Notify settings first. See *4.2.6 Alarm Notification*.

[Camera Adjustment] Allows you to adjust the image quality.

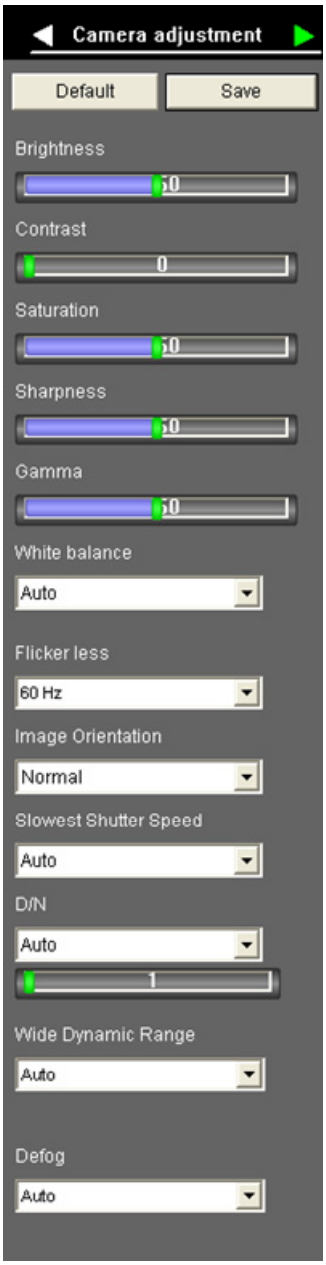


Figure 4-6

- **Brightness:** Adjusts the brightness of the image.
- **Contrast:** Adjusts the relative differences between one pixel and the next.
- **Saturation:** Adjusts the saturation of the image.
- **Sharpness:** Adjusts the sharpness of the image.
- **Gamma:** Adjusts the relative proportions of bright and dark areas.
- **White balance:** The camera automatically adjusts the color to be closest to the image you are viewing. You can choose one of the environments: **Outdoor**, **Tungsten Lamp** and **Fluorescent**. You can also choose **Manual** to adjust the white balance manually.
- **Flicker less:** The camera automatically matches the frequency of your camera's imager to the frequency of indoor light sources, e.g. fluorescent lighting. You can also select 50 Hz or 60 Hz manually. If these don't match, faint light and dark bars may appear in your images. Check the power utility to determine which frequency is used.
- **Image Orientation:** Changes the image orientation on the Live View window.
- **Slowest Shutter Speed:** The shortest duration that the image sensor is exposed to light. The minimum shutter speed ranges from 1/5 to 1/8000 sec. Under low light conditions, a faster shutter speed will lower color quality and image clarity. For manual shutter speed, the options are between 1/5 and 1/8000 sec. For automatic shutter speed, select **Auto**.
- **D/N:** Sets the Day/Night mode of the camera. When **Auto** is selected, you can use the slider to adjust the sensitivity level of the light sensor. The higher the value, the more sensitive the camera is to light. For details, see *5.1.1 Video Settings*.
- **Wide Dynamic Range**: Adjusts and generates clear live view when the scene contains very bright and very dark areas at the same time. Select **Auto (Strong)** to bring out details in the darks areas of the scene, select **Auto (Weak)** to bring out less detail in the dark area and at the same time keep the bright areas from overexposure, or select **Auto (Normal)** for a balanced effect. Select **Close** to disable the function.
- **Defog**: Select **Auto** to automatically enhance the visibility of images. Select **Close** to disable the function.

[GPS] For details see *5.5.2 GPS Maps Setting*.

[Download] Allows you to install the programs from the hard drive.

4.2.3 Snapshot of a Live Video

To take a snapshot of live video, follow these steps:

1. Click the **Snapshot** button (No. 5, Figure 4-3). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and select **JPEG** or **BMP** as **Save as Type**. You may also choose whether to display the name and date stamps on the image.
3. Click the **Save** button to save the image in the local computer.

4.2.4 Video Recording

You can record live video for a certain period of time to your local computer.

1. Click the **File Save** button (No. 6, Figure 4-3). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and move the **Time period** scroll bar to specify the time length of the video clip from 1 to 5 minutes.
3. Click the **Save** button to start recording.
4. To stop recording, click the **Stop** button (No. 2, Figure 4-3).

4.2.5 Picture-in-Picture and Picture-and-Picture View

Two types of close-up views are available to provide clear and detailed images of the surveillance area: **Picture-in-Picture (PIP)** and **Picture-and Picture (PAP)**. After entering the live view window, the image is displayed in PIP mode by default.

Picture-in-Picture View

With the Picture in Picture (PIP) view, you can crop the video to get a close-up view or zoom in on the video.

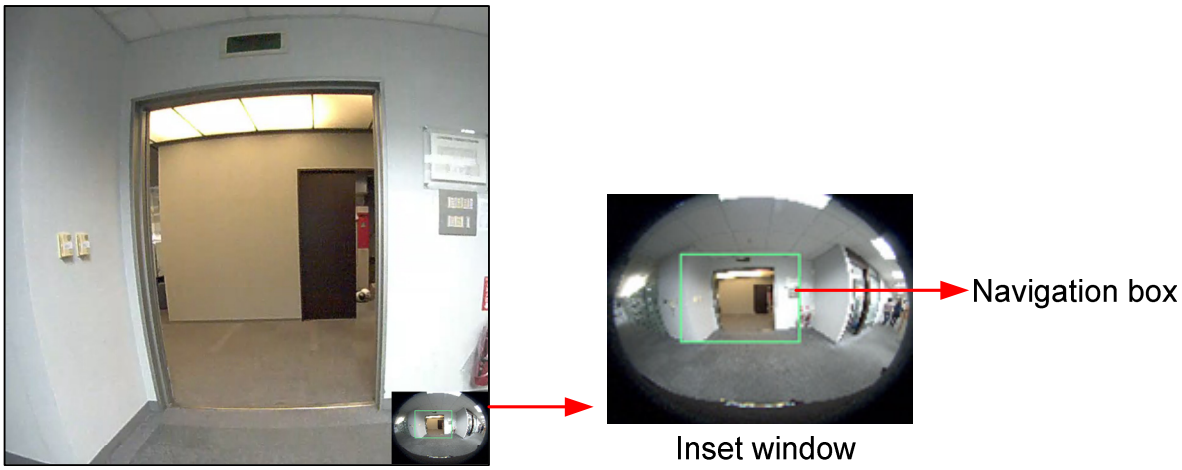


Figure 4-7

1. Right-click the live view and select **PIP**. An inset window appears.
2. Click the inset window. A navigation box appears.
3. Move the navigation box around in the inset window to have a close-up view of the selected area.
4. To adjust the navigation box size, move the cursor to any of the box corners, and enlarge or diminish the box.
5. To exit the PIP view, right-click the image and click **PIP** again.

Picture-and-Picture View

With the Picture and Picture (PAP) view, you can create a split video effect with multiple close-up views on the image. A total of 7 close-up views can be defined.

Figure 4-8

1. Right-click the live view and select **PAP**. Three inset windows appear at the bottom.
2. Draw a navigation box on the image, and this selected area is immediately reflected in one inset window. Up to seven navigation boxes can be drawn on the image.
3. To adjust a navigation box size, move the cursor to any of the box corners, and enlarge or diminish the box.
4. To move a navigation box to another area on the image, drag it to that area.
5. To change the frame color of the navigation box or hide the box, right-click the image, select **Mega Pixel Setting** and click one of these options:
   - **Display Focus Area of PAP Mode:** Displays or hides the navigation boxes on the image.
   - **Set Color of Focus Area:** Changes the color of the box frames.
6. To delete a navigation box, right-click the desired box, select **Focus Area of PAP Mode** and click **Delete**.
7. To exit the PAP view, right-click the image and click **PAP** again.

4.2.6 Alarm Notification

After motion detection, you can be alerted by a pop-up live video and view up to four captured images.

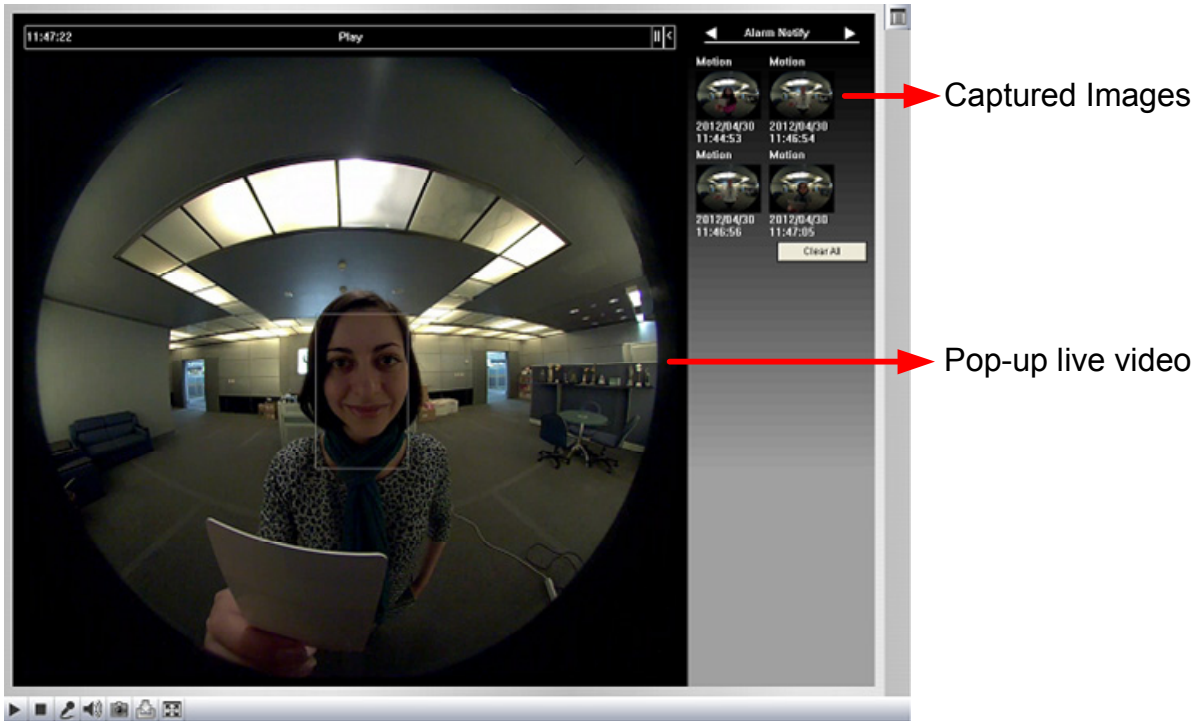


Figure 4-9

To configure this function, click the **Show System Menu** button (No. 8, Figure 4-3), and select **Alarm Notify**. This dialog box appears.

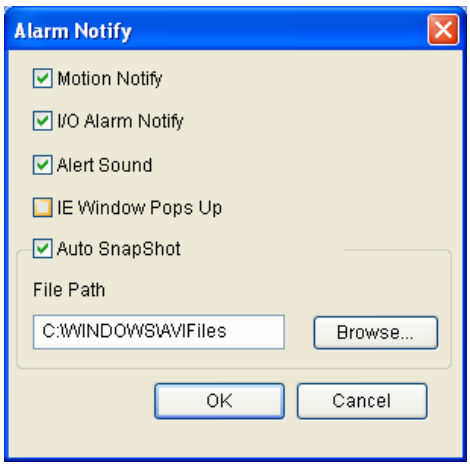


Figure 4-10

- **Motion Notify:** Once motion is detected, the captured images are displayed on the control panel of the Live View window.

- **I/O Alarm Notify:** This function is not supported on GV-CR420.
- **Alert Sound:** Activates the computer alarm on motion detection.
- **Auto Snapshot:** The snapshot of live video is taken every 5 seconds upon motion detection.
  - **File Path:** Assigns a file path to save the snapshots.

Note: The Administrator can adjust the motion detection area by using the Motion Detection function. See *5.1.2 Motion Detection* for more details.

4.2.7 Video and Audio Configuration

You can enable the microphone and speaker for two-way audio communication and adjust the number of frames to keep for live view buffer.

Click the **Show System Menu** button (No. 8, Figure 4-3), and select **Video and Audio Configuration**.

- **Camera:** Sets the number of frames to keep in live view buffer. Keeping more frames in live view buffer can ensure a smooth live view, but the live view will be delayed for the number of frames specified and not be presented in real time.

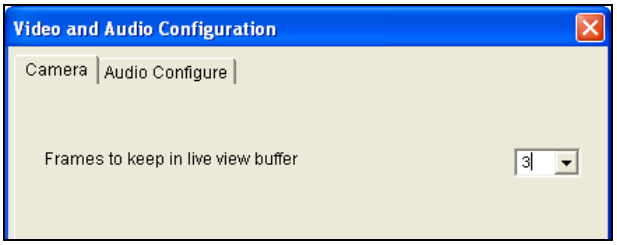


Figure 4-11

- **Audio Configure:** You can enable the microphone and speaker and adjust the audio volume.

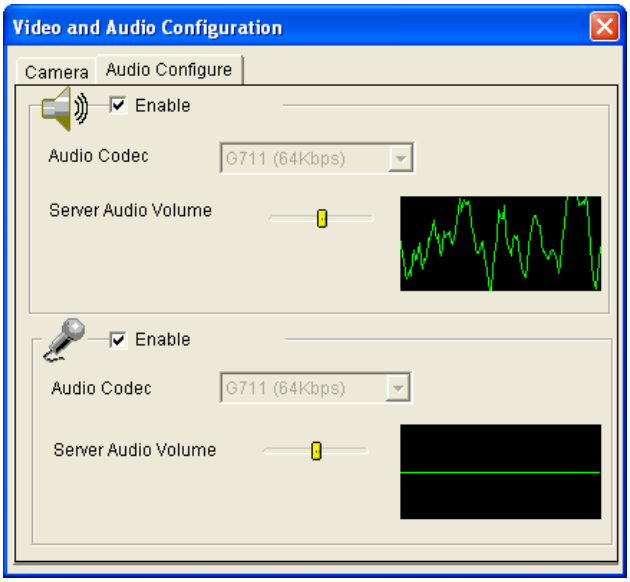


Figure 4-12

4.2.8 Remote Configuration

You can upgrade firmware over the network in Remote Configuration. Click the **Show System Menu** button (No. 8, Figure 4-3), and select **Remote Config**. The Remote Config dialog box will appear.

[Firmware Upgrade] In this tab, you can upgrade the firmware over the network. For details, see *Chapter 6 Advanced Applications*.

4.2.9 Camera Name Display

To display the camera name on the image, click the **Show System Menu** button (No. 8, Figure 4-3), and select **Show Camera Name**.

4.2.10 Image Enhancement

To enhance the image quality of live video, click the **Show System Menu** button (No. 8, Figure 4-3), and select **Image Enhance**. This dialog box appears.

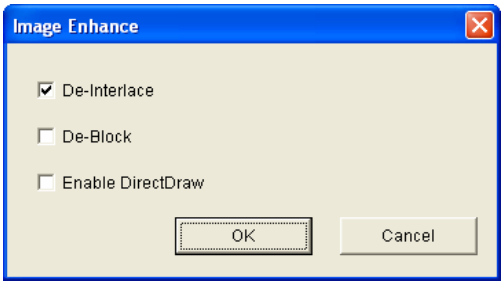


Figure 4-13

- **De-Interlace:** Coverts the interlaced video into non-interlaced video.
- **De-Block:** Removes the block-like artifacts from low-quality and highly compressed video.
- **Enable DirectDraw:** Activates the DirectDraw function.

4.2.11 Network Status

To view the network status, in the left menu, click **Network** and select **Status**.

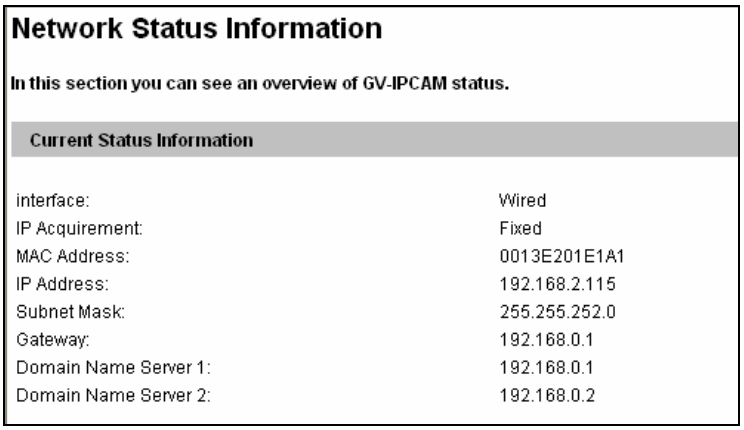


Figure 4-14

Chapter 5 Administrator Mode

The Administrator can access system configuration through the network. The following configuration categories are available: **Video and Motion**, **Events and Alerts**, **Monitoring**, **Network** and **Management**.

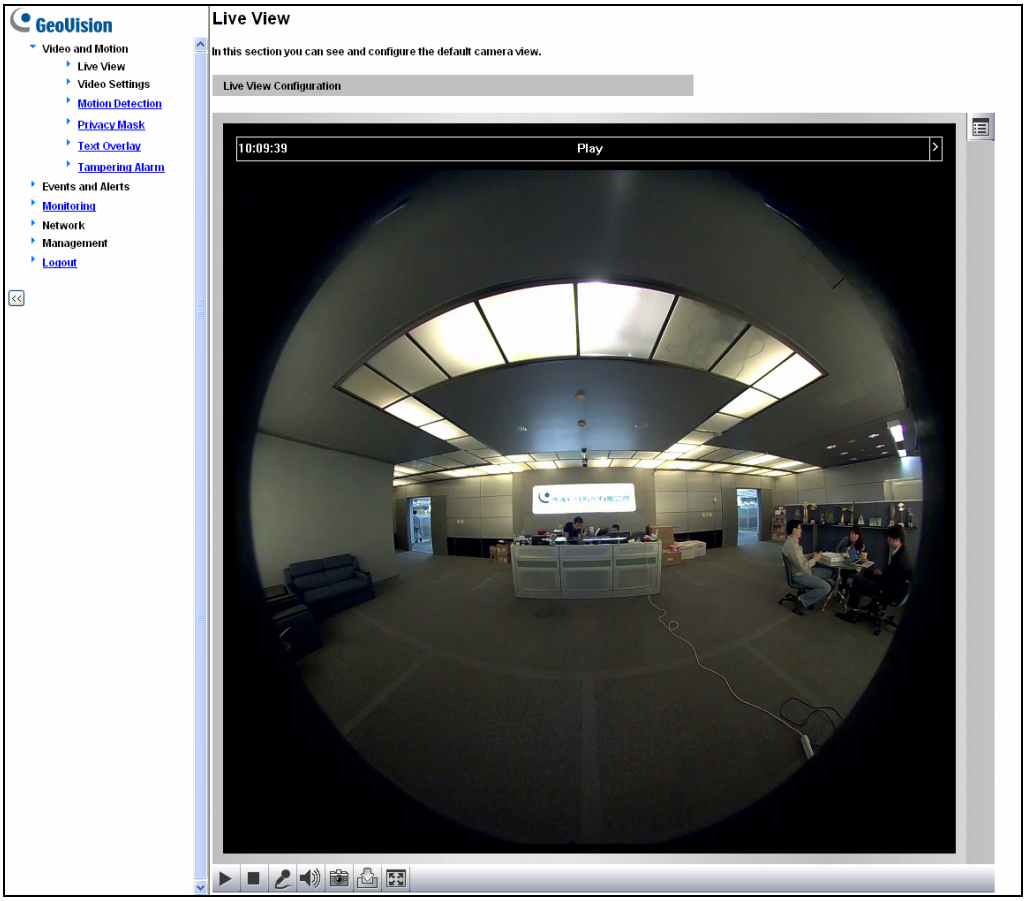


Figure 5-1

List of Menu Options

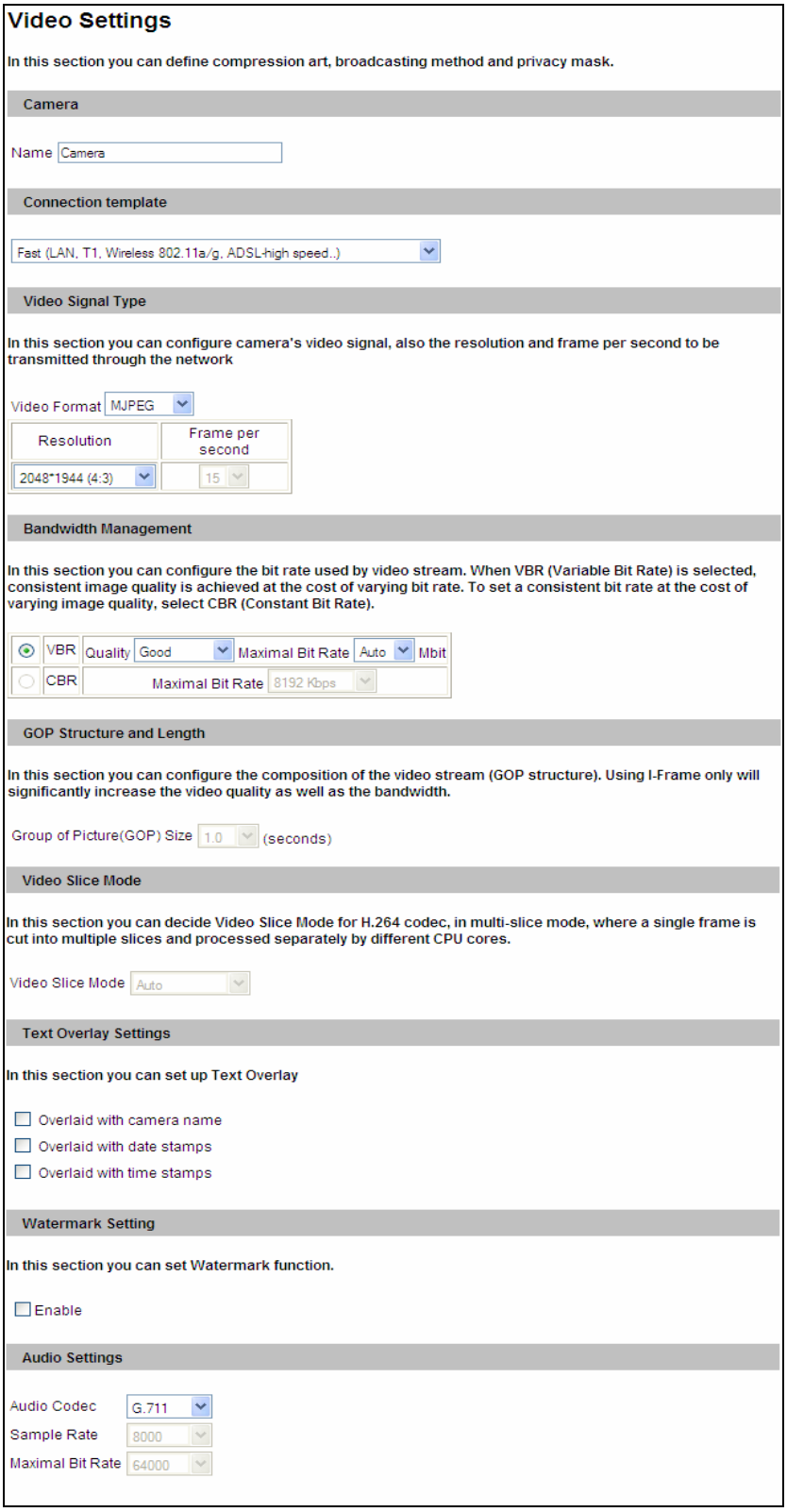
Find the topic of interest by referring to the section number prefixed to each option.

5.1 Video and Motion	5.1.1 Video Settings 5.1.2 Motion Detection 5.1.3 Privacy Mask 5.1.4 Text Overlay 5.1.5 Tampering Alarm
5.2 Events and Alerts	5.2.1 Email 5.2.2 FTP 5.2.3 Center V2 5.2.4 VSM 5.2.5 Video Gateway / Recording Server 5.2.6 RTSP
5.3 Monitoring	
5.4 Network	5.4.1 LAN 5.4.2 Advanced TCP/IP 5.4.3 IP Filtering 5.4.4 SNMP Setting
5.5 Management	5.5.1 Date and Time Settings 5.5.2 GPS Maps Settings 5.5.3 User Account 5.5.4 Log Information 5.5.5 Tools

5.1 Video & Motion

This section includes the video image settings and how the images can be managed by using Motion Detection, Privacy Mask, Text Overlay, and Tampering Alarm.

5.1.1 Video Settings


Video Settings
In this section you can define compression art, broadcasting method and privacy mask.
Camera
Name Camera
Connection template
Fast (LAN, T1, Wireless 802.11a/g, ADSL-high speed..)
Video Signal Type
In this section you can configure camera's video signal, also the resolution and frame per second to be transmitted through the network
Video Format MJPEG
Resolution
Frame per second
2048*1944 (4:3)
15
Bandwidth Management
In this section you can configure the bit rate used by video stream. When VBR (Variable Bit Rate) is selected, consistent image quality is achieved at the cost of varying bit rate. To set a consistent bit rate at the cost of varying image quality, select CBR (Constant Bit Rate).
VBR Quality Good Maximal Bit Rate Auto Mbit
CBR Maximal Bit Rate 8192 Kbps
GOP Structure and Length
In this section you can configure the composition of the video stream (GOP structure). Using I-Frame only will significantly increase the video quality as well as the bandwidth.
Group of Picture(GOP) Size 1.0 (seconds)
Video Slice Mode
In this section you can decide Video Slice Mode for H.264 codec, in multi-slice mode, where a single frame is cut into multiple slices and processed separately by different CPU cores.
Video Slice Mode Auto
Text Overlay Settings
In this section you can set up Text Overlay
Overlaid with camera name
Overlaid with date stamps
Overlaid with time stamps
Watermark Setting
In this section you can set Watermark function.
Enable
Audio Settings
Audio Codec G.711
Sample Rate 8000
Maximal Bit Rate 64000

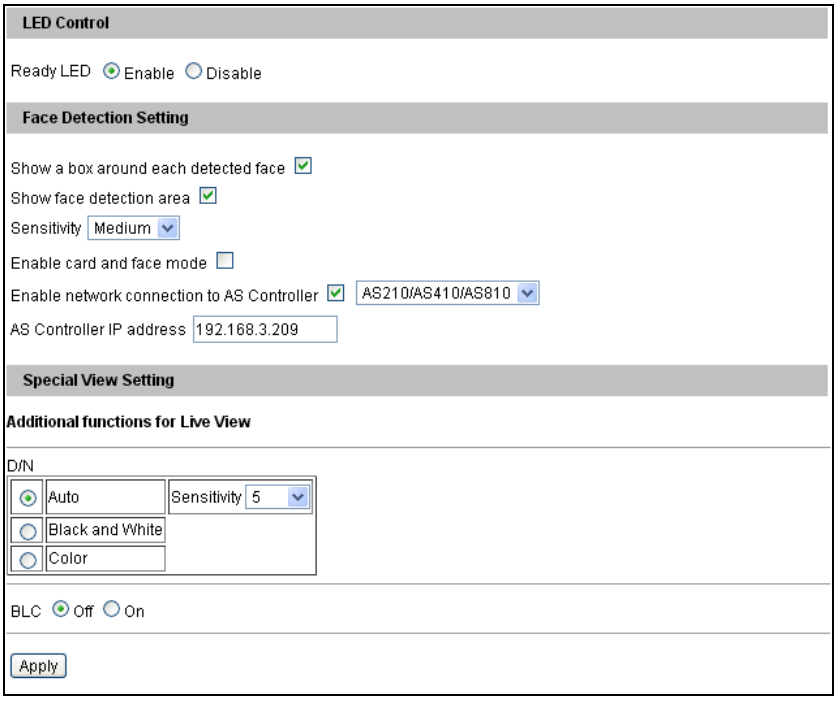


Figure 5-2

[Name]

Rename the video stream. The camera name will appear on the Live View. To display the name of the video stream on the Live View window, see *4.2.9 Camera Name Display*.

[Connection Template]

Select the type of your network connection. The recommended video resolution, frame rate, bandwidth and GOP size for each connection type will automatically be selected unless **Customized** is selected.

[Video Signal Type]

The codec options, resolutions and maximum frame rates are listed as below:

Streams	Codec Options	Image Resolution	Maximum Frame Rate
Stream 1	H.264, MJPEG	2048 x 1944	15 fps
Stream 2	H.264, MJPEG	640 x 480, 320 x 240	15 fps

[Bandwidth Management]

When using H.264, you can select constant bitrate or variable birate to control the bandwidth usage.

- **VBR (Variable Bitrate):** The quality of the video stream is kept as constant as possible at the cost of a varying bitrate. The bandwidth is used much more efficiently than a

comparable CBR. You can set a limit to the bit rate by specifying a **Maximal Bit Rate**. Set the image quality to one of the 5 standards: **Standard, Fair, Good**, **Great**, and **Excellent.**

- **CBR (Constant Bitrate):** CBR is used to achieve a specific bitrate by varying the quality of the stream. Use the **Maximal Bit Rate** drop-down list to select a bitrate.

[GOP Structure and Length]

Use the **Group of Picture(GOP) Size** drop-down list to set the number of frames between every key frame. This option is only available when H.264 is selected for codec. The limit is 1 key frame for every 30 frames.

[Video Slice Mode]

Corrects the display mode of the camera when it is displayed on a third-party NVR/DVR software and the live view is incomplete or broken. Select **Single Slice** or **Multi Slice** to display the live view. The default is **Auto**.

[Text Overlay Settings]

Overlay the image with camera name, date, or time.

- **Overlaid with camera name:** Includes camera names on live and recorded videos.
- **Overlaid with date stamps:** Includes date stamps on live and recorded videos.
- **Overlaid with time stamps:** Includes time stamps on live and recorded videos.

[Watermark] Enable this option to watermark all recordings. The watermark allows you to verify whether the recorded video has been tampered with. See *6.4 Verifying Watermark*.

[Audio Settings] The default settings are audio codec AAC, sample rate 16000 and maximal bit rate 64000. The Sample Rate and Maximal Bit Rate settings are only available with the audio codec AAC.

- **Audio Codec:** Select AAC or G.711 using the drop-down list.
- **Sample Rate:** Select the frequency for audio sampling. The higher the frequency, the better the audio quality.
- **Maximal Bit Rate:** Select the maximum audio bit rate. The higher the bit rate, the better the audio quality.

[LED Control] Select **Disable** if you do not want to use the Ready LED (No. 7, Figure 1-3).

[Face Detection Setting]

- **Show a box around each detected face:** Select this option to draw a box around each detected face on camera view.
- **Show face detection area:** Show face detection area on camera view to indicate the area where face detection is supported.
- **Sensitivity:** Select a sensitivity level for face detection.
- **Enable card and face mode:** Select this option to require a card to be presented and a face to be detected before access is granted. The LED Indicator will flash red if the camera reader fails to detect the face.
- **Enable network connection to AS Controller:** Select this option and use the drop-down list to select the controller to enable the network connection between the camera reader and GV-AS Controller.
- **AS Controller IP address:** Type the IP address of the GV-AS Controller. This option is only available when the **Enable network connection to AS Controller** option is enabled. Connecting using domain name is not supported.

[Special View Setting]

- **D/N:** Sets the Day/Night mode of the camera.
  - **Auto:** Select **Auto** for the camera to detect the amount of light present and automatically switch to monochrome in a poorly-lit scene. Use the drop-down list to adjust the sensitivity level of light sensor from 1 to 5. The higher the value, the more sensitive the camera is to light.
  - **Black and White:** Select this option for the live view to be in monochrome.
  - **Color:** Select this option for the live view to be in color.

[BLC] Enable backlight compensation to adjust the exposure when the subject is positioned in front of a bright light source.

5.1.2 Motion Detection

Motion detection is used to generate an alarm whenever movement occurs in the video image. You can configure up to 8 areas with different sensitivity values for motion detection.

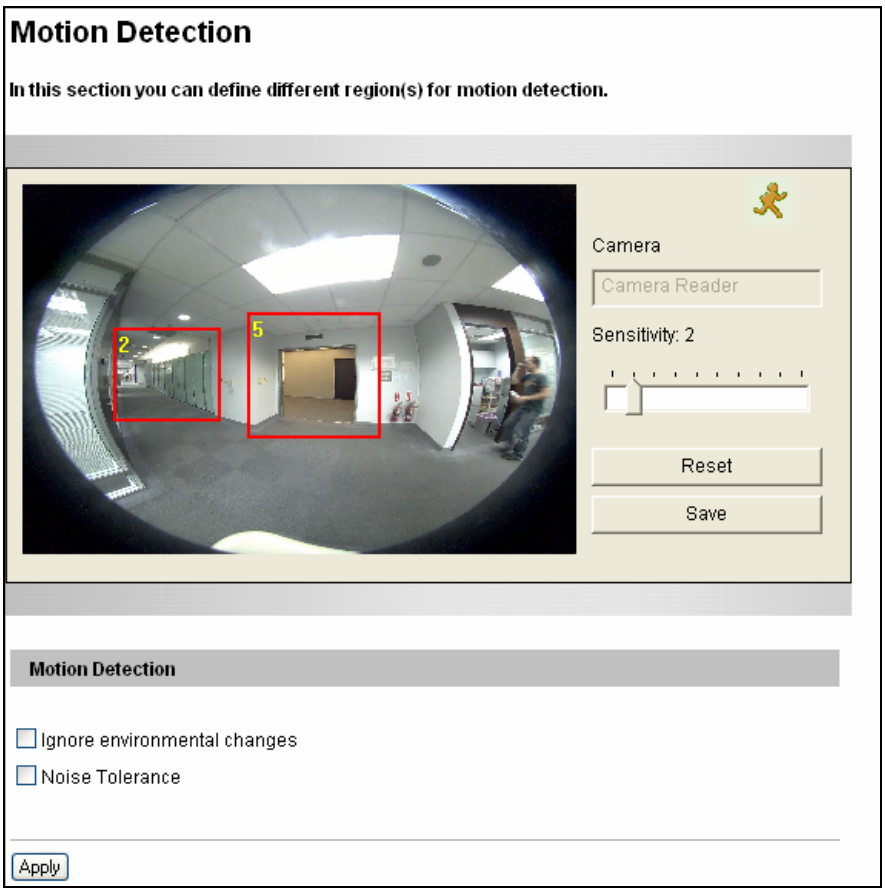


Figure 5-3

The motion detection function is disabled by default. Follow the steps below to set up and enable motion detection.

1. Select the desired sensitivity level by moving the slider. The higher the value, the more sensitive the camera is to motion.
2. Drag an area on the image. Click **Add** when you are prompted to confirm the setting.
3. To create several areas with different sensitivity values, repeat Steps 2 and 3.
4. Click **Save** to save the above settings.
5. Under Motion Detection section, select the following options to reduce false alarm.
   - **Ignore environmental changes:** Ignore environmental changes in the camera view such as rain or snow.
   - **Noise Tolerance:** Ignore video noise when light changes.

5.1.3 Privacy Mask

The Privacy Mask can block out sensitive areas from view, covering the areas with dark boxes in both live view and recorded clips. This feature is ideal for locations where displays, keyboard sequences (e.g. passwords), and confidential information might be visible.

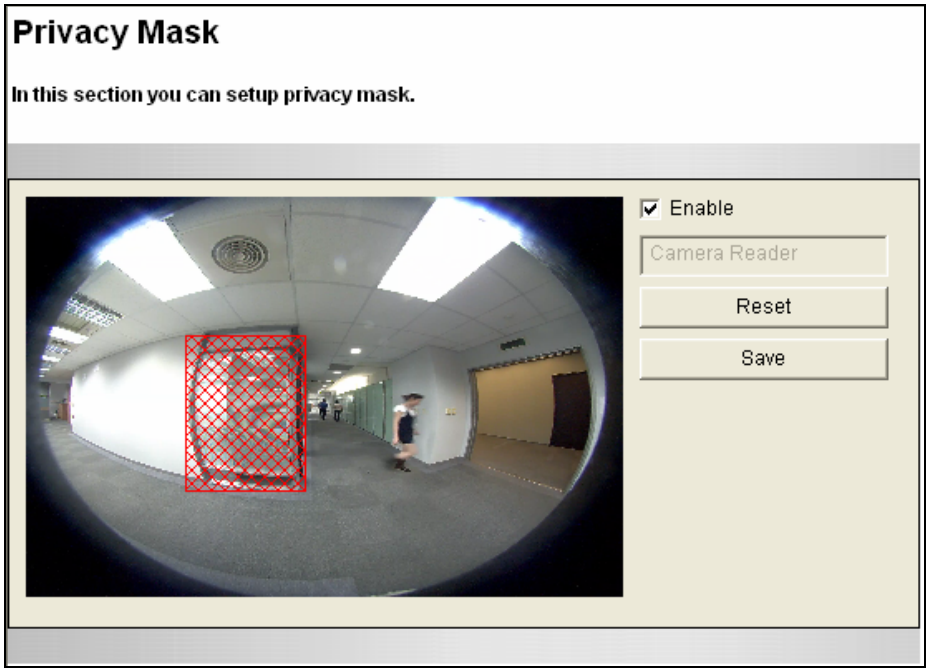


Figure 5-4

1. Select the **Enable** option.
2. Drag the area(s) where you want to block out on the image. Click **Add** when you are prompted to confirm the setting.
3. Click the **Save** button to save the settings.

5.1.4 Text Overlay

The Text Overlay allows you to overlay any text in any place on the camera view. Up to 16 text messages can be created on one camera view. The overlaid text will be saved in the recordings.

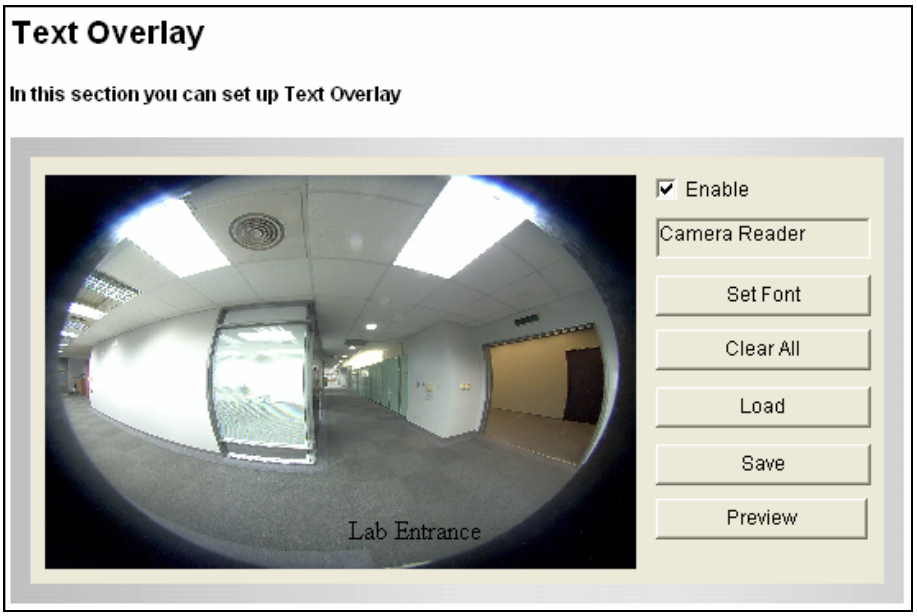


Figure 5-5

1. Select the font, font style and font size in a pop-up window.
2. Select the **Enable** option.
3. Click any place on the image. This dialog box appears.

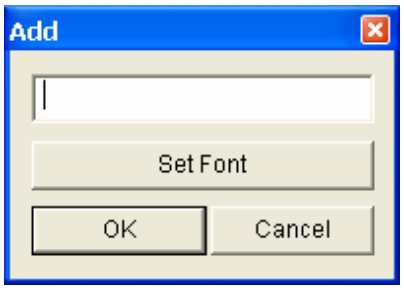


Figure 5-6

4. Type the desired text, and click **OK**. The text is overlaid on the image.
5. Drag the overlaid text to a desired place on the image.
6. Click **Set Font** to modify the font settings.
7. Click **Save** to apply the settings, or click **Load** (Undo) to revert to the last saved setting.
8. Click **Preview** to see how the text will appear on the image. Click **Close** to end the preview.

5.1.5 Tampering Alarm

The Tampering Alarm is used to detect when the camera is being physically tampered with. An e-mail alert can be generated when the camera is moved, covered up, or out of focus. To enable the tampering alarm, first enable the e-mail setting and select **Tampering Alarm**. See *5.2.1 E-Mail.*

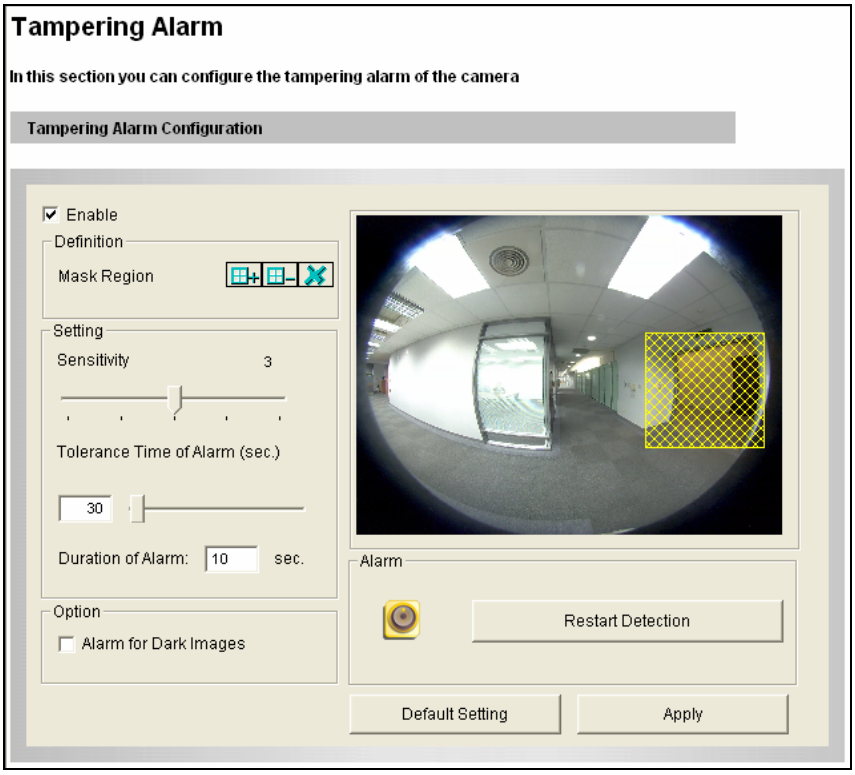


Figure 5-7

To configure the tampering alarm:

1. Select **Enable**.
2. If you want the camera to ignore any movement or scene change in certain areas, click the button to drag areas on the camera view.
3. Select the desired detection sensitivity by moving the slider. The higher the value, the more sensitive the camera is to scene changes.
4. In the **Tolerance Time of Alarm** field, specify the time length allowed for scene changes before an alarm is generated.
5. In the **Duration of Alarm** field, specify the interval between each alarm notification.
6. To trigger an alarm when the scene turns dark, e.g. the lens of camera has been covered, select **Alarm for Dark Images**.
7. Click **Apply** to save all the settings.

5.2 Events & Alerts

The Administrator can set up the following alert methods to receive notifications when motion is detected or when the camera is tampered with.

1. Send a captured still image by e-mail or FTP.
2. Notify Center Monitoring Station, Center V2 or VSM, by video or text alerts.

To activate the above alert methods, you must set the following functions in advance:

- Motion Detection (See *5.1.2 Motion Detection*)
- Tampering Alarm (See *5.1.5 Tampering Alarm*)
- For e-mail and FTP alerts, it is required to start monitoring (See *5.3 Monitoring*).

5.2.1 E-mail

After a motion or tampering event, the camera can send an e-mail to a remote user containing a captured still image.

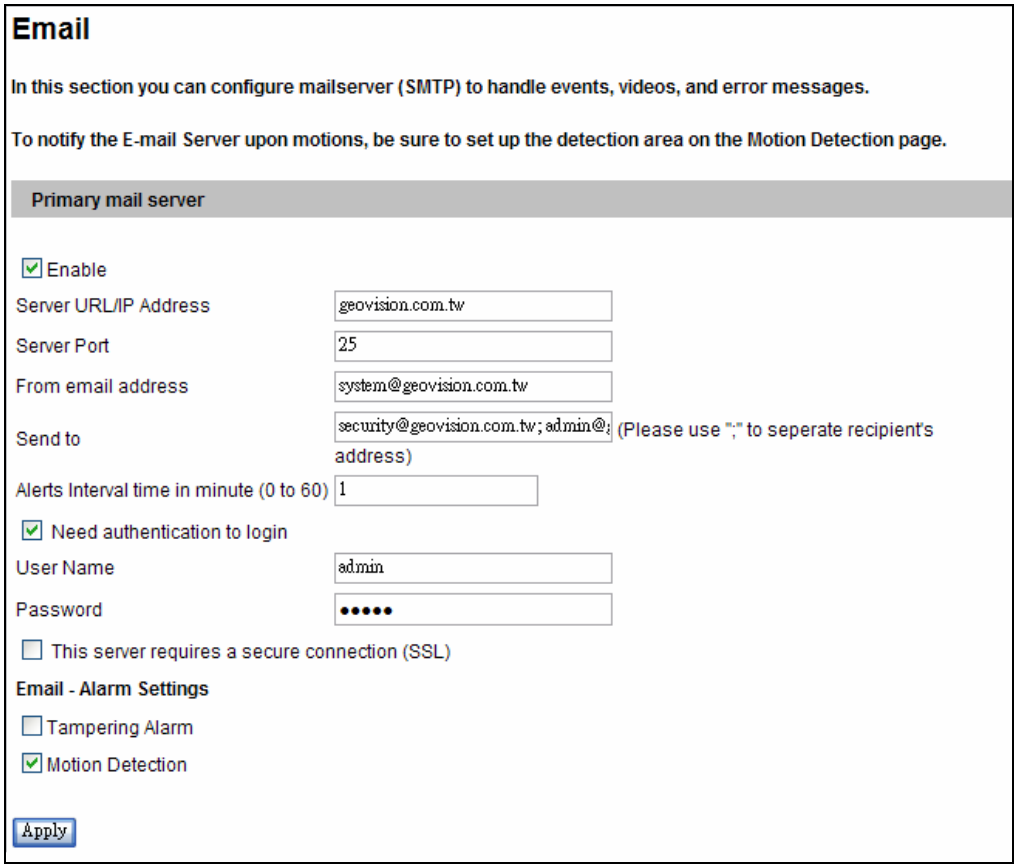


Figure 5-8

To enable the e-mail functions:

1. Select **Enable** to set up e-mail notifications.
2. **Server URL/IP Address:** Type the SMTP Server's URL address or IP address.
3. **Server Port:** Type the SMTP Server's port number. Or keep the default value 25.
4. **From email address:** Type the sender's e-mail address.
5. **Send to:** Type the e-mail address(s) you want to send alerts to.
6. **Alerts interval time in minute:** Specify the interval between e-mail alerts. The interval can be between 0 and 60 minutes. The option is useful for frequent event occurrence. Any event triggers during the interval period will be ignored.
7. If the SMTP Server needs authentication, select **Need authentication to login** and type a valid **Username** and **Password** to log in the SMTP server. If the SMTP Server needs a secure connection (SSL), select **This server requires a secure connection**.
8. **Email-Alarm Settings:** Select to automatically send an e-mail alert upon motion detection or tampering alarm.
9. Click **Apply**.
10. In the left menu, select **Monitoring** and click the **Start** button to activate e-mail and FTP alert.

Important: To send e-mail alert upon motion or tampering alarm, be sure to set up the detection area on the Motion Detection page and enable the Tampering Alarm function. For details, see *5.1.2 Motion Detection* and *5.1.5 Tampering Alarm*.

5.2.2 FTP

You can also send the captured still image to a remote FTP server for alerts.

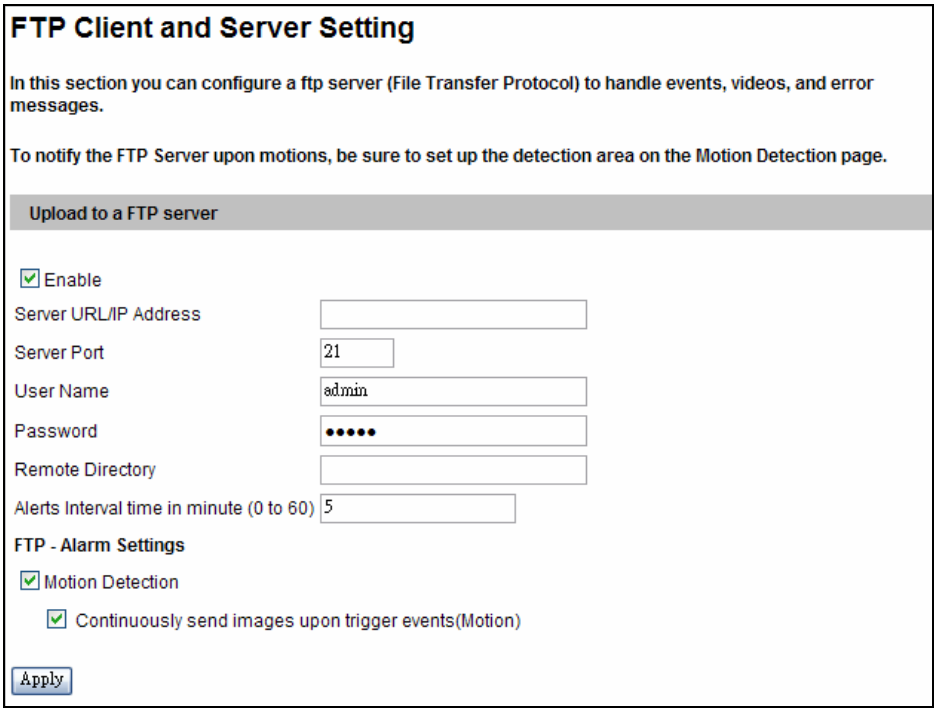

FTP Client and Server Setting
In this section you can configure a ftp server (File Transfer Protocol) to handle events, videos, and error messages.
To notify the FTP Server upon motions, be sure to set up the detection area on the Motion Detection page.
Upload to a FTP server
Enable
Server URL/IP Address
Server Port
21
User Name
admin
Password
Remote Directory
Alerts Interval time in minute (0 to 60)
5
FTP - Alarm Settings
Motion Detection
Continuously send images upon trigger events(Motion)
Apply

Figure 5-9

To enable the e-mail functions:

1. Select **Enable** to set up the FTP function.
2. **Server URL/IP Address:** Type the URL address or IP address of the FTP Server.
3. **Server Port:** Type the port number of the FTP Server. Or keep the default value 21.
4. Type the **Username** and **Password** of the FTP Server.
5. **Remote Directory:** Type the name of the storage folder on the FTP Server.
6. **Alerts interval time in minute:** Specify the interval between FTP alerts. The interval can be between 0 and 60 minutes. The option is useful for frequent event occurrence. Any event triggers during the interval period will be ignored.
7. **FTP-Alarm Settings:** Select to automatically send a snapshot to the FTP Server upon motion detection. Select **Continuously send images upon trigger events (Motion)** to upload a series of snapshots to the FTP Server when motion is detected.
8. Click **Apply**.
9. In the left menu, select **Monitoring** and click the **Start** button to activate e-mail and FTP alert.

Important: To send FTP alert upon motions, be sure to set up the detection area on the Motion Detection page. For details, see *5.1.2 Motion Detection*.

5.2.3 Center V2

After a motion detection event, the central monitoring station Center V2 can be notified by live videos and text alerts. For the live monitoring through Center V2, you must already have a subscriber account on Center V2. The camera can connect with up to two Center V2.

Important: To notify the Center V2 Server upon motions, be sure to set up the detection area on the Motion Detection page.

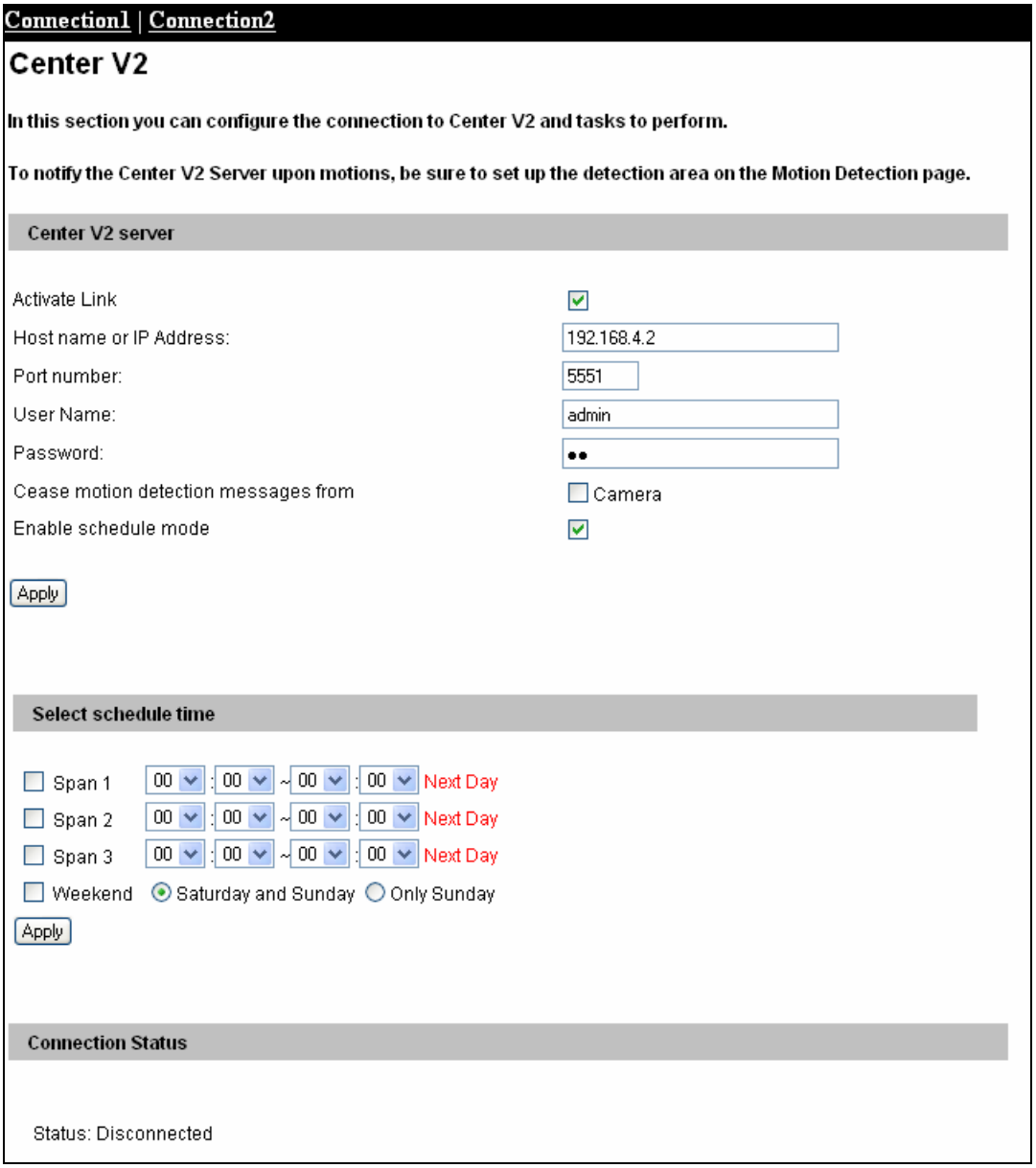


Figure 5-10

To enable the Center V2 connection:

1. **Activate Link:** Enable the monitoring through Center V2.
2. **Host Name or IP Address:** Type the host name or IP address of Center V2.
3. **Port Number:** Match the port to **Port 2** on Center V2. Or keep the default value 5551. For details, see *8.1 Center V2.*
4. **User Name:** Type a valid user name to log into Center V2.
5. **Password:** Type a valid password to log into Center V2.
6. Click **Apply.** The Connection Status should display “Connected” and the connected time.
7. To establish the connection to the second Center V2, click the **Connection 2** tab and repeat the above steps for setup.

These options can also be found on this Center V2 setting page:

- **Cease motion detection messages from:** Stops notifying Center V2 of motion-triggered events.
- **Enable schedule mode:** Starts the monitoring through Center V2 based on the schedule you set in the **Select Schedule Time** section.

[Select Schedule Time]

- **Span 1- Span 3:** Specify the time to start connecting to and monitoring through Center V2. Each day can be divided into 3 time spans, shown as Span 1, Span2, and Span 3. The time span settings apply to Monday through Friday.
- **Weekend:** Enable this option to start recording all day on the weekend and select whether your weekend includes **Saturday and Sunday** or **Only Sunday**.

For related settings to activate the monitoring through Center V2, see *5.1.2 Motion Detection* and *8.1 Center V2.*

5.2.4 VSM

After a motion detection event, the central monitoring station VSM can get notified by text alerts. For the live monitoring through VSM, you must already have a subscriber account on VSM. The camera can be connected with up to two VSM.

Important: To notify the VSM upon motions, be sure to set up the detection area on the Motion Detection page.

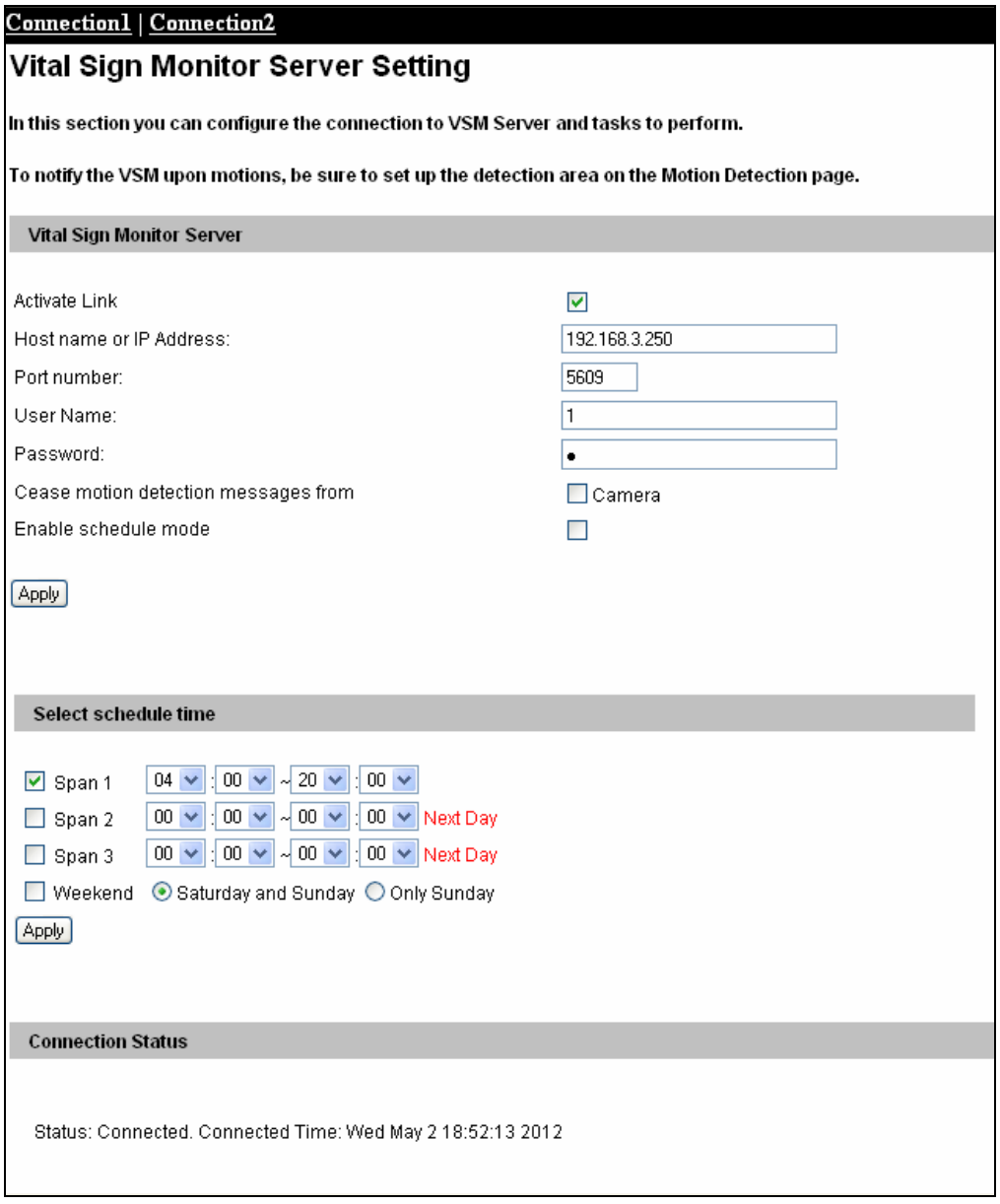

Connection1 | Connection2
Vital Sign Monitor Server Setting
In this section you can configure the connection to VSM Server and tasks to perform.
To notify the VSM upon motions, be sure to set up the detection area on the Motion Detection page.
Vital Sign Monitor Server
Activate Link
Host name or IP Address:
192.168.3.250
Port number:
5609
User Name:
1
Password:
Cease motion detection messages from
Camera
Enable schedule mode
Apply
Select schedule time
Span 1
04 : 00 ~ 20 : 00
Span 2
00 : 00 ~ 00 : 00 Next Day
Span 3
00 : 00 ~ 00 : 00 Next Day
Weekend
Saturday and Sunday
Only Sunday
Apply
Connection Status
Status: Connected. Connected Time: Wed May 2 18:52:13 2012

Figure 5-11

To enable the VSM connection:

1. **Activate Link:** Enable the monitoring through VSM.
2. **Host Name or IP Address:** Type the host name or IP address of VSM.
3. **Port Number:** Match the port to **Port 2** on VSM. Or keep the default value 5609. For details, see *8.2 VSM.*
4. **User Name:** Type a valid user name to log into VSM.
5. **Password:** Type a valid password to log into VSM.
6. Click **Apply**. The Connection Status should display “Connected” and connected time.
7. To establish the connection to the second VSM, click the **Connection 2** tab and repeat the above steps for setup.

These options you can also find on this VSM setting page:

- **Cease motion detection messages from:** Stops notifying VSM of motion-triggered events.
- **Enable schedule mode:** Starts the monitoring through VSM based on the schedule you set in the **Select Schedule Time** section. Refer to *5.2.3 Center V2* for the same settings.

For related settings to activate the monitoring through VSM, see *5.1.2 Motion Detection*, and *8.2 VSM*.

5.2.5 Video Gateway / Recording Server

The GV-Video Gateway / GV-Recording Server is a video streaming server designed for large-scale video surveillance deployments. The GV-Video Gateway / GV-Recording Server (with recording capability) can receive up to 128 channels from various IP video devices, and distribute up to 300 channels to its clients. With GV-Video Gateway / GV-Recording Server, the desired frame rate can be ensured while the CPU loading and bandwidth usage of the IP video devices are significantly reduced.

The camera reader can be connected with up to two GV-Video Gateway / GV-Recording Server. To send the video images to the GV-Video Gateway or GV-Recording Server, follow the steps below.

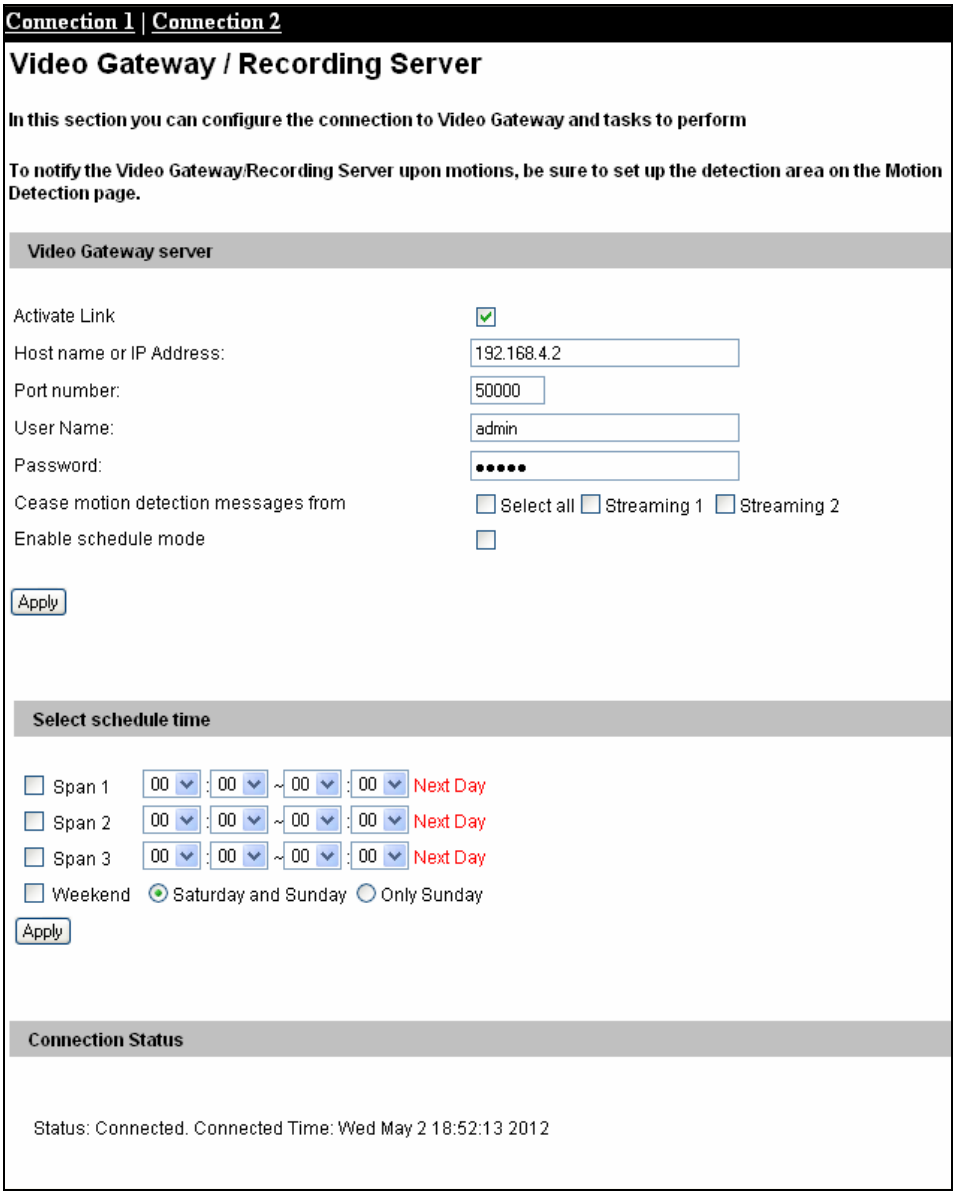


Figure 5-12

1. **Activate Link:** Enable the connection to the GV-Video Gateway / GV-Recording Server.
2. **Host Name or IP Address:** Type the host name or IP address of the GV-Video Gateway / GV-Recording Server.
3. **Port Number:** Match the communication port on the GV-Video Gateway / GV-Recording Server or keep the default value 50000.
4. **User Name:** Type a valid user name to log into the GV-Video Gateway / GV-Recording Server.
5. **Password:** Type a valid password to log into the GV-Video Gateway / GV-Recording Server.
6. **Enable schedule mode:** Enable the GV-Video Gateway / GV-Recording Server connection on the schedule you set in the **Select Schedule Time** section. Refer to *5.2.3 Center V2* for the same settings.
7. Click **Apply**. The Connection Status should display “Connected” and the connected time.
8. To establish the connection to the second GV-Video Gateway / GV-Recording Server, click the **Connection 2** tab and repeat the above steps for setup.

Note: The **Cease motion detection messages from** function is not functional.

5.2.6 RTSP

The RTSP Server enables RTSP protocol for video streaming.

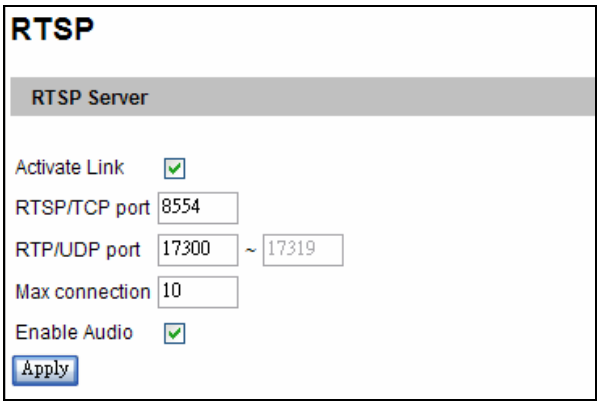


Figure 5-13

- **Activate Link:** Enable the RTSP protocol.
- **RTSP/TCP Port:** Keep the default value 8554, or modify it if necessary.
- **RTP/UDP Port:** Keep the default range from 17300 to 17319, or modify it if necessary. The number of ports for use is limited to 20.
- **Max Connection:** Set the maximum number of connections to the camera reader.
- **Enable Audio:** Turns audio streaming on or off.

For details on the RTSP command, see *RTSP Protocol Support* in Appendix B.

5.3 Monitoring

To receive email and FTP alert, click **Start** to activate e-mail and FTP alert.

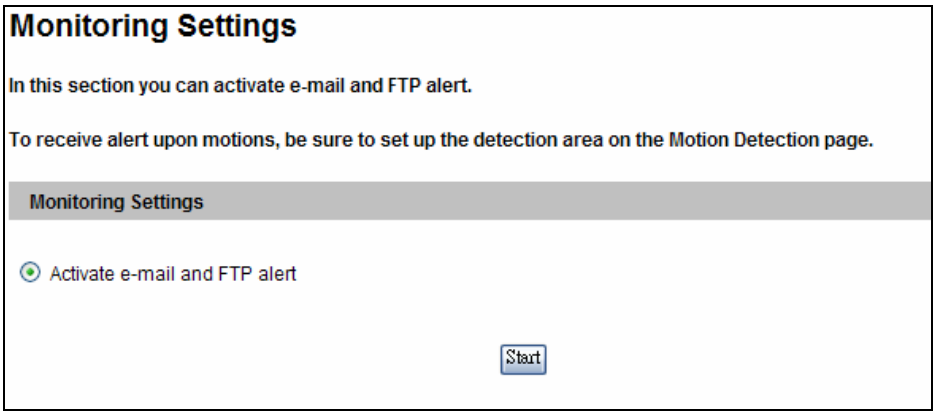

Monitoring Settings
In this section you can activate e-mail and FTP alert.
To receive alert upon motions, be sure to set up the detection area on the Motion Detection page.
Monitoring Settings
Activate e-mail and FTP alert
Start

Figure 5-14

5.4 Network

The Network section includes some basic but important network configurations that enable the camera to be connected to a TCP/IP network.

5.4.1 LAN

According to your network environment, select among Static IP, DHCP and PPPoE.

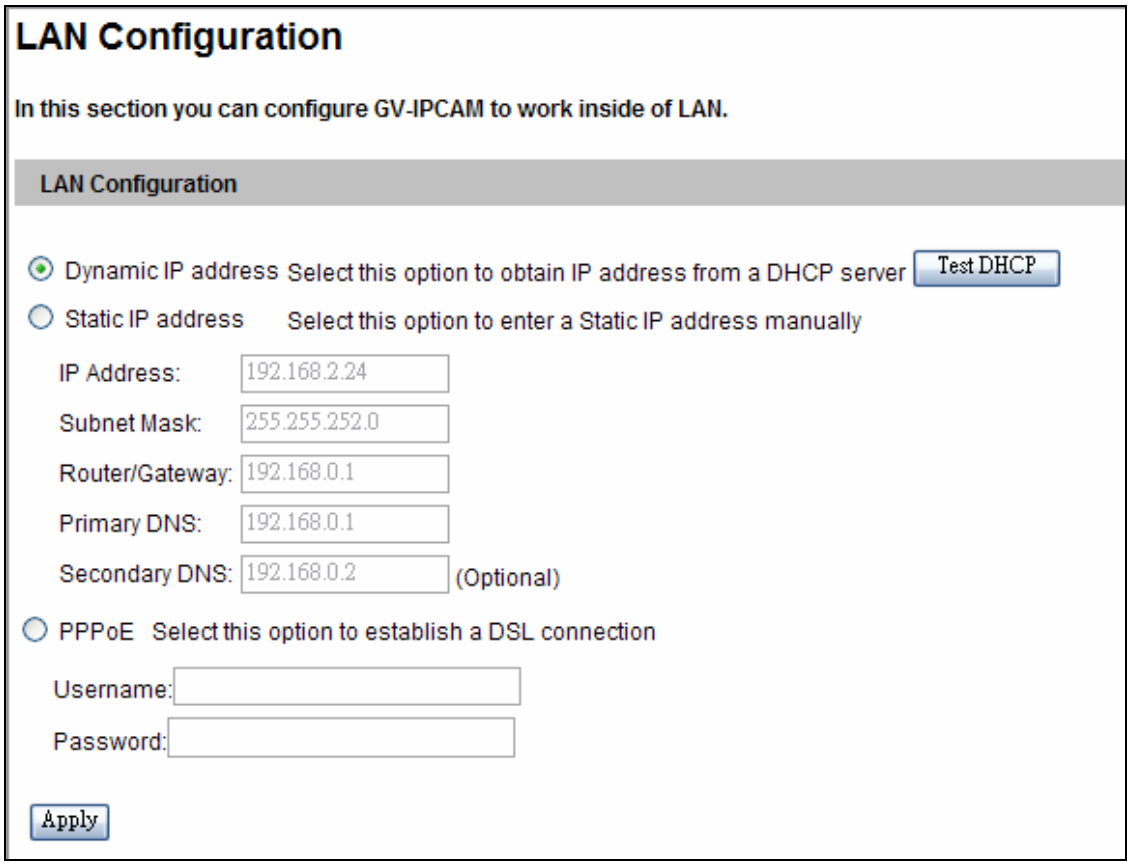

LAN Configuration
In this section you can configure GV-IPCAM to work inside of LAN.
LAN Configuration
Dynamic IP address Select this option to obtain IP address from a DHCP server
Test DHCP
Static IP address Select this option to enter a Static IP address manually
IP Address: 192.168.2.24
Subnet Mask: 255.255.252.0
Router/Gateway: 192.168.0.1
Primary DNS: 192.168.0.1
Secondary DNS: 192.168.0.2 (Optional)
PPPoE Select this option to establish a DSL connection
Username:
Password:
Apply

Figure 5-15

[LAN Configuration]

- **Dynamic IP address:** The network environment has a DHCP server which will automatically assign a dynamic IP address to the camera. Click the **Test DHCP** to see the currently assigned IP address or look up the address using GV-IP Device Utility.

- **Static IP address:** Assign a static IP or fixed IP to the camera. Type the camera's IP address, Subnet Mask, Router/Gateway, Primary DNS server and Secondary DNS server.

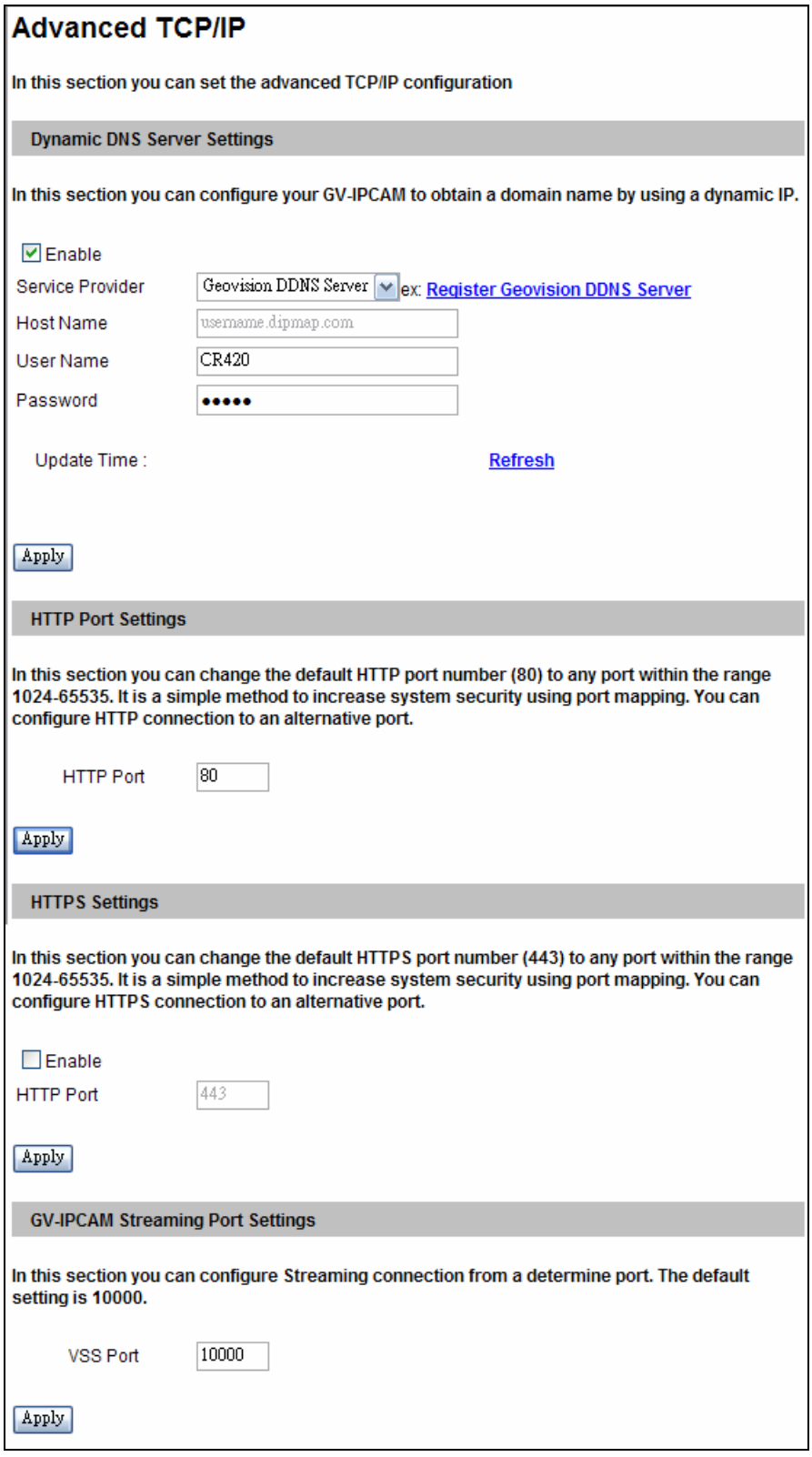
Parameters	Default
IP address	192.168.0.10
Subnet Mask	255.255.255.0
Router/Gateway	192.168.0.1
Primary DNS server	192.168.0.1
Secondary DNS server	192.168.0.2

- **PPPoE:** The network environment is xDSL connection. Type the Username and Password provided by ISP to establish the connection. If you use the xDSL connection with dynamic IP addresses, first use the DDNS function to obtain a domain name linking to the camera's changing IP address.

For details on Dynamic DNS Server Settings*, see 5.4.2 Advanced TCP/IP.*

5.4.2 Advanced TCP/IP

This section introduces the advanced TCP/IP settings, including DDNS Server, HTTP port, streaming port, UPnP and QoS.


Advanced TCP/IP
In this section you can set the advanced TCP/IP configuration
Dynamic DNS Server Settings
In this section you can configure your GV-IPCAM to obtain a domain name by using a dynamic IP.
Enable
Service Provider
Geovision DDNS Server
ex: Register Geovision DDNS Server
Host Name
username.dipmap.com
User Name
CR420
Password
Update Time :
Refresh
Apply
HTTP Port Settings
In this section you can change the default HTTP port number (80) to any port within the range 1024-65535. It is a simple method to increase system security using port mapping. You can configure HTTP connection to an alternative port.
HTTP Port
80
Apply
HTTPS Settings
In this section you can change the default HTTPS port number (443) to any port within the range 1024-65535. It is a simple method to increase system security using port mapping. You can configure HTTPS connection to an alternative port.
Enable
HTTP Port
443
Apply
GV-IPCAM Streaming Port Settings
In this section you can configure Streaming connection from a determine port. The default setting is 10000.
VSS Port
10000
Apply

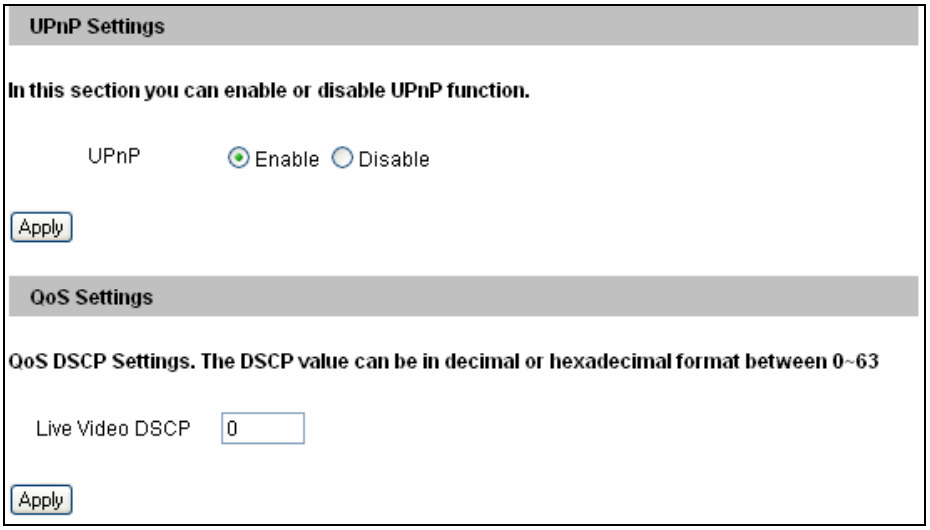


Figure 5-16

[Dynamic DNS Server Settings]

DDNS (Dynamic Domain Name System) provides a convenient way of accessing the camera when using a dynamic IP. DDNS assigns a domain name to the camera, so that the Administrator does not need to go through the trouble of checking if the IP address assigned by DHCP Server or ISP (in xDSL connection) has changed.

Before enabling the following DDNS function, the Administrator should have applied for a Host Name from the DDNS service provider's website. There are 2 providers listed in the camera: GeoVision DDNS Server and DynDNS.org.

To enable the DDNS function:

1. **Enable:** Enable the DDNS function.
2. **Service Provider:** Select the DDNS service provider you have registered with.
3. **Host Name:** Type the host name used to link to the camera. For users of GeoVision DDNS Server, it is unnecessary to fill the field because the system will detect the host name automatically.
4. **User Name:** Type the user name used to enable the service from the DDNS.
5. **Password:** Type the password used to enable the service from the DDNS.
6. Click **Apply**.

[HTTP Port Settings]

The HTTP port enables connecting the camera to the web. For security integration, the Administrator can hide the server from the general HTTP port by changing the default HTTP port of 80 to a different port number within the range of 1024 through 65535.

[HTTPS Settings]

By enabling the HTTPS settings, you can access the camera through a secure protocol. You can change the default HTTPS port 443 to a different port number within the range of 1024 through 65535. Click **Apply**. The Web interface will be restarted automatically and you will need to log in again.

[GV-IPCAM Streaming Port Settings]

The VSS port enables connecting the camera to the GV-System. The default setting is 10000.

[UPnP Settings]

UPnP (Universal Plug & Play) is a networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. It means that they are listed in the network devices table for the operating system (such as Windows XP) supported by this function. Enabling this function, you can connect to the camera directly by clicking on the camera listed in the network devices table.

[QoS Settings] The Quality of Service (QoS) is a bandwidth control mechanism that guarantees delay-sensitive data flows such as voice and video streams, obtain a certain amount of bandwidth to keep the streaming smooth.

To apply QoS to the camera reader, all network routers must support QoS and QoS must be enabled on these devices. To enable the QoS on the camera, enter a Differentiated Services Code Point (DSCP) value. This value is a field in an IP packet that enables different levels of services for the network traffic. When the video stream from the camera reaches a router, the DSCP value will tell the router what service level to be applied, e.g. the bandwidth amount. This value ranges from 0 to 63 in decimal format. The default value is 0, meaning QoS is disabled.

5.4.3 IP Filtering

The Administrator can set IP filtering to restrict access to the camera.

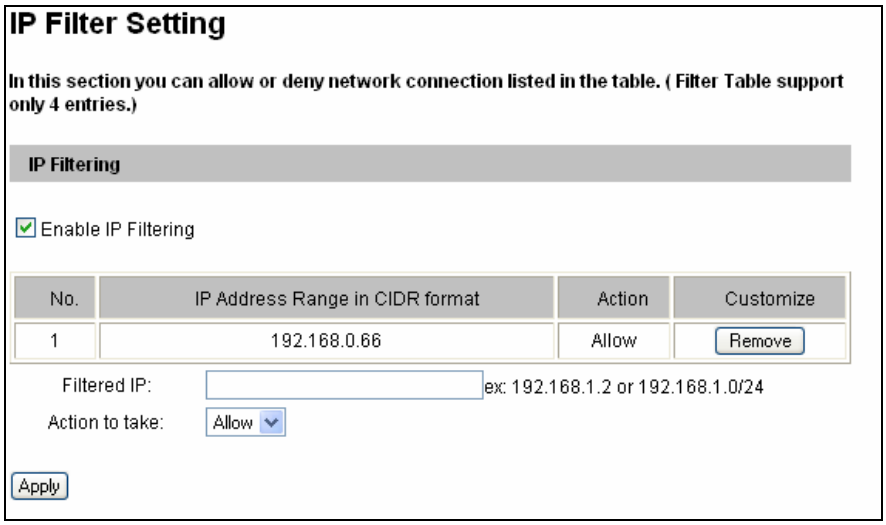


Figure 5-17

To enable the IP Filter function:

1. **Enable IP Filtering:** Enable the IP Filtering function.
2. **Filtered IP:** Type the IP address you want to restrict the access.
3. **Action to take:** Select to **Allow** or **Deny** the IP address(es) you have specified.
4. Click **Apply**.

5.4.4 SNMP Setting

The Simple Network Management Protocol (SNMP) allows you to monitor the status of the camera with SNMP network management software.

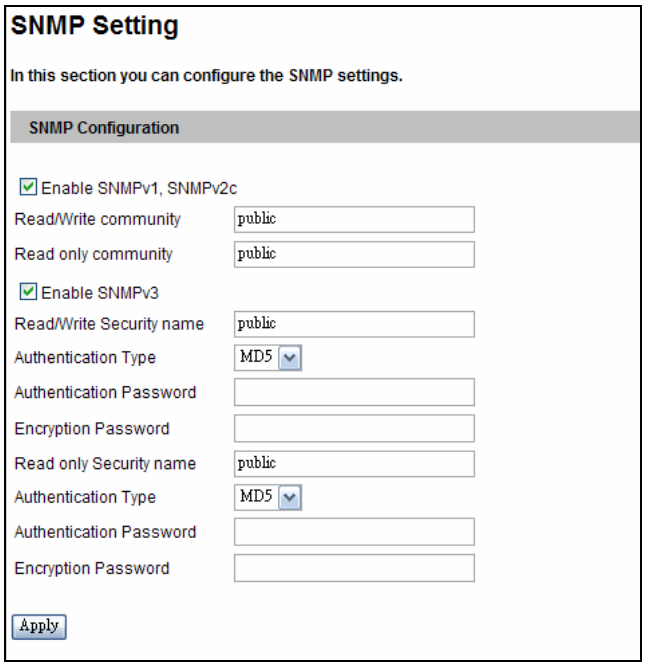


Figure 5-18

To set up the SNMP settings:

1. Select **Enable SNMPv1 SNMPv2c** to enable the function.
2. To enable access to **Read/Write community**, type a community string. This will serve as a password to allow read and write access to the camera from the SNMP software.
3. To enable **Read only community**, type a community string to allow read only access to the camera from the SNMP software.
4. For a more secured connection, select **Enable SNMPv3** to enable SNMP version 3.
5. To enable access to SNMPv3 Read/Write community, type a **Read/Write Security name**.
6. Select an **Authentication Type** to use for SNMP requests.
7. Type the **Authentication Password** and **Encryption Password**. You will need to type these passwords in the SNMP software to be able to access the camera.
8. To enable access to SNMPv3 Read only community, type a **Read only Security name** and follow steps 6 – 7.
9. Click **Apply** to save the settings.

5.5 Management

The Management section includes the settings of data and time, GPS maps, and user account. Also you can view the firmware version and execute certain system operations.

5.5.1 Date and Time Settings

The date and time settings are used for date and time stamps on the image.

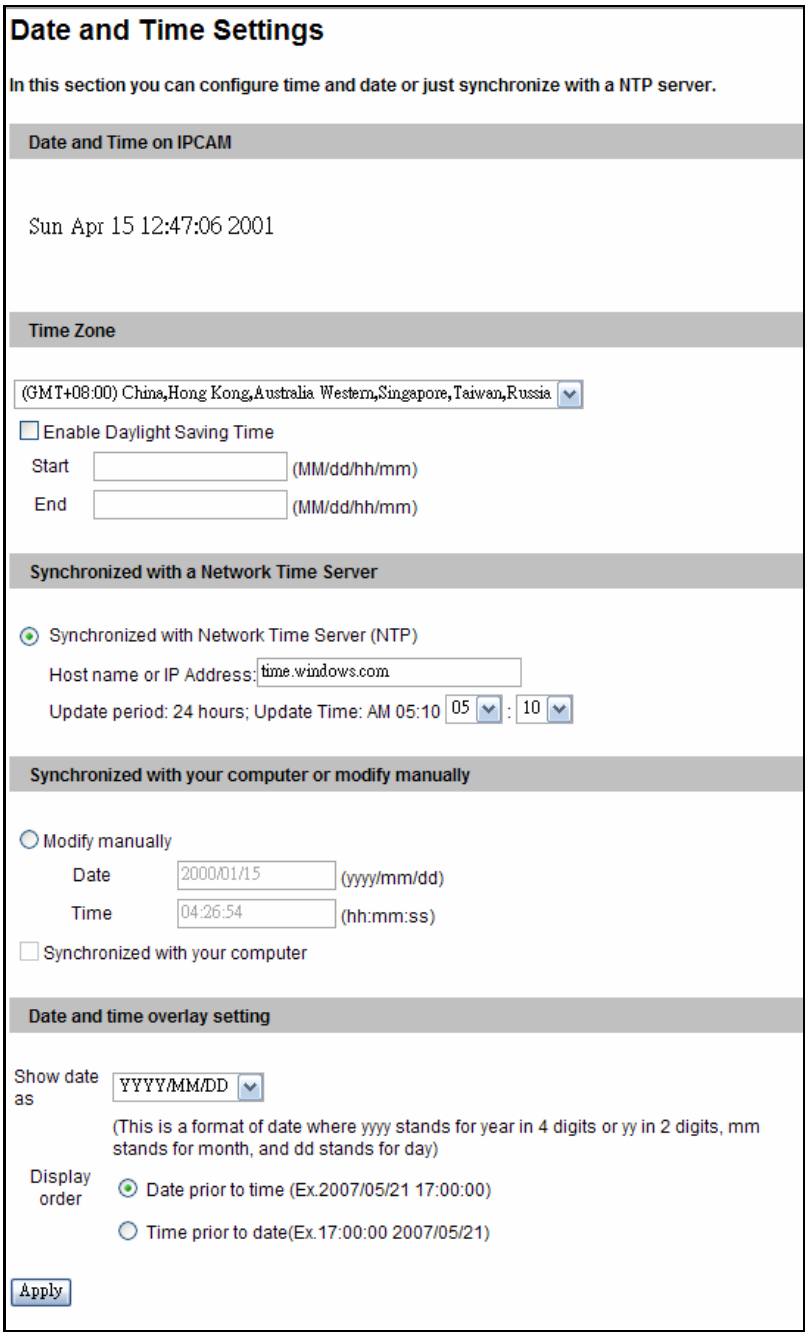

Date and Time Settings
In this section you can configure time and date or just synchronize with a NTP server.
Date and Time on IPCAM
Sun Apr 15 12:47:06 2001
Time Zone
(GMT+08:00) China,Hong Kong,Australia Western,Singapore,Taiwan,Russia
Enable Daylight Saving Time
Start
(MM/dd/hh/mm)
End
(MM/dd/hh/mm)
Synchronized with a Network Time Server
Synchronized with Network Time Server (NTP)
Host name or IP Address: time.windows.com
Update period: 24 hours; Update Time: AM 05:10 05 : 10
Synchronized with your computer or modify manually
Modify manually
Date 2000/01/15 (yyyy/mm/dd)
Time 04:26:54 (hh:mm:ss)
Synchronized with your computer
Date and time overlay setting
Show date as YYYY/MM/DD
(This is a format of date where yyyy stands for year in 4 digits or yy in 2 digits, mm stands for month, and dd stands for day)
Display order
Date prior to time (Ex.2007/05/21 17:00:00)
Time prior to date(Ex.17:00:00 2007/05/21)
Apply

Figure 5-19

[Date & Time on IPCAM] Displays the current date and time on the camera.

[Time Zone] Sets the time zone for local settings. Select **Enable Daylight Saving Time** to automatically adjust the camera for daylight saving time. Type the Start Time and End Time to enable the daylight saving function. To automatically synchronize the Daylight Saving Time with the GV-System, see *7.1.1 Customizing the Basic Settings*.

[Synchronized with a Time Server] By default, the camera uses the timeserver of time.windows.com to automatically update its internal clock every 24 hours at the Update Time you specified. You can also change the host name or IP setting to the timeserver of interest.

[Synchronized with your computer or manually] Manually changes the camera's date and time. Or, synchronize the camera's date and time with those of the local computer.

[Date and time overlay setting] Select the display format of date and time stamps on the image. For this function to work, you must also enable the **Overlaid with date stamps** and **Overlaid with time stamps** options in Figure 5-2.

5.5.2 GPS Maps Settings

The Maps Settings allows you to see the location of your camera on Google maps, without a GPS device.

To see the location of your camera on maps:

1. It is required to sign up for a Google Maps API key before using the Google Maps. Click **Link to the Google Maps API**.

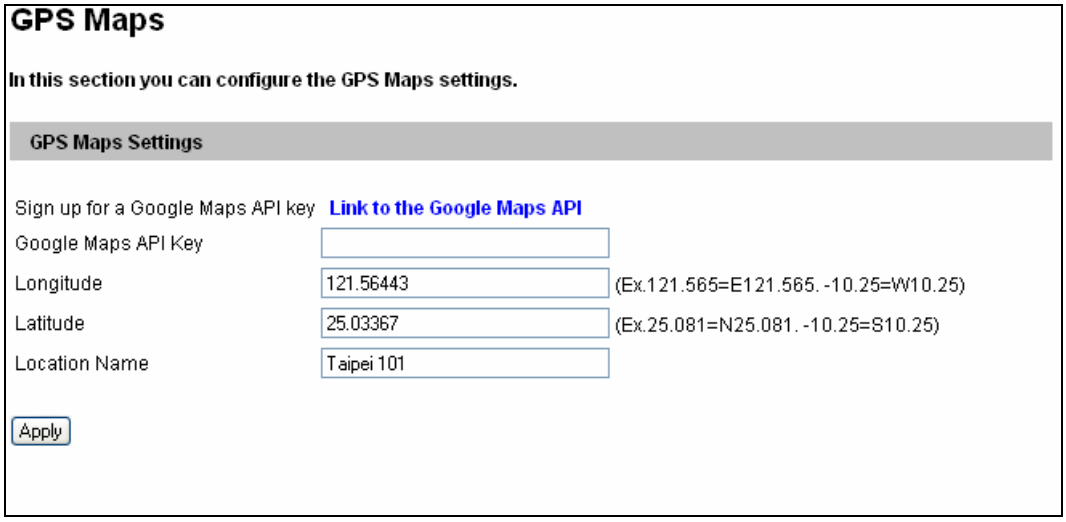


Figure 5-20

2. Type the registered Maps API Key, the longitude and latitude of your camera, and location name. Click **Apply** to enable this function.
3. Open the control panel of the Live View window.

Figure 5-21

4. Click **Open**. A warning message appears.

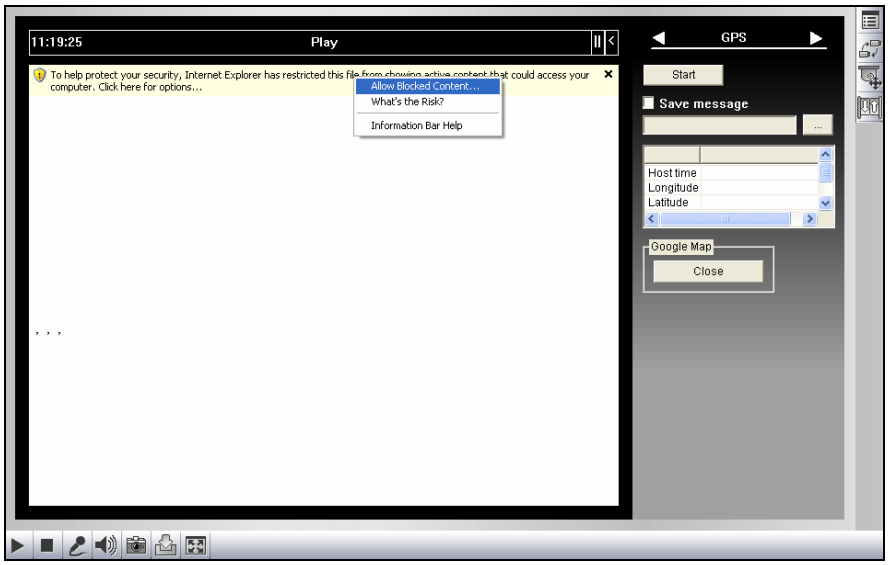


Figure 5-22

5. Right-click the warning message and select **Allow Blocked Content**. The map is displayed. The icon indicates the location of your camera. At the upper right corner you have options to view different map formats, such as Satellite and Hybrid.

Figure 5-23

5.5.3 User Account

You can change the login name and password of Administrator and Guest.

- The default Administrator login name and password are **admin**.
- The default Guest login name and password are **guest**.
- To allow a Guest user to log in without entering name and password, select **Disable authentication for guest account**.
- To remain logged in after reboot, select **Disable auto logout after reboot**.

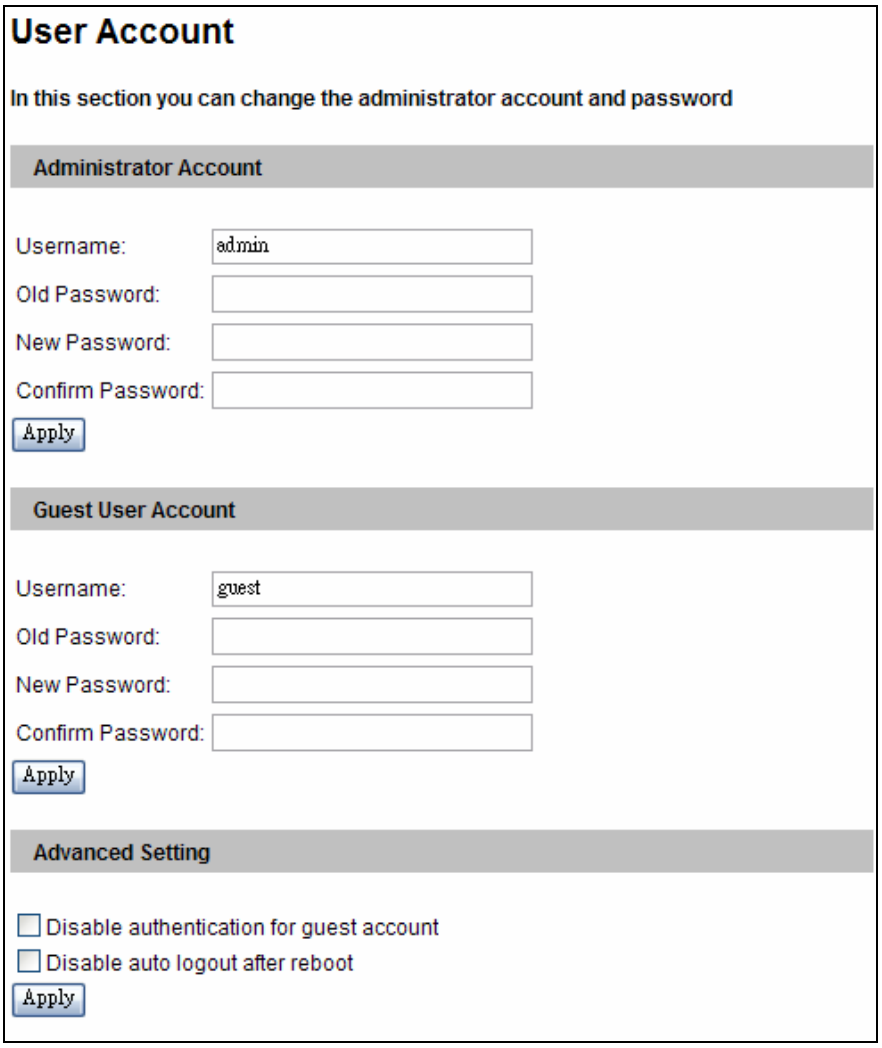


Figure 5-24

5.5.4 Log Information

The log information contains dump data that is used by service personnel for analyzing problems.

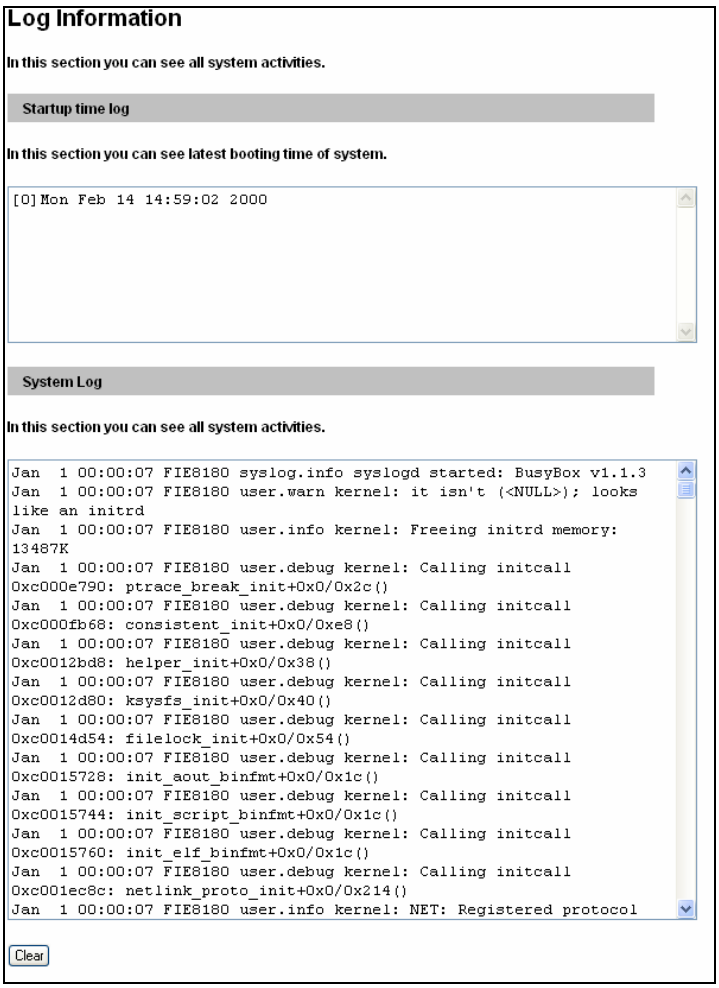

Log Information
In this section you can see all system activities.
Startup time log
In this section you can see latest booting time of system.
[0]Mon Feb 14 14:59:02 2000
System Log
In this section you can see all system activities.
Jan 1 00:00:07 FIE8180 syslog.info syslogd started: BusyBox v1.1.3
Jan 1 00:00:07 FIE8180 user.warn kernel: it isn't (<NULL>); looks like an initrd
Jan 1 00:00:07 FIE8180 user.info kernel: Freeing initrd memory: 13487K
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc000e790: ptrace_break_init+0x0/0x2c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc000fb68: consistent_init+0x0/0xe8()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0012bd8: helper_init+0x0/0x38()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0012d80: ksysfs_init+0x0/0x40()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0014d54: filelock_init+0x0/0x54()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0015728: init_aout_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0015744: init_script_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc0015760: init_elf_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall 0xc001ec8c: netlink_proto_init+0x0/0x214()
Jan 1 00:00:07 FIE8180 user.info kernel: NET: Registered protocol
Clear

Figure 5-25

5.5.5 Tools

This section allows you to execute certain system operations and view the firmware version.

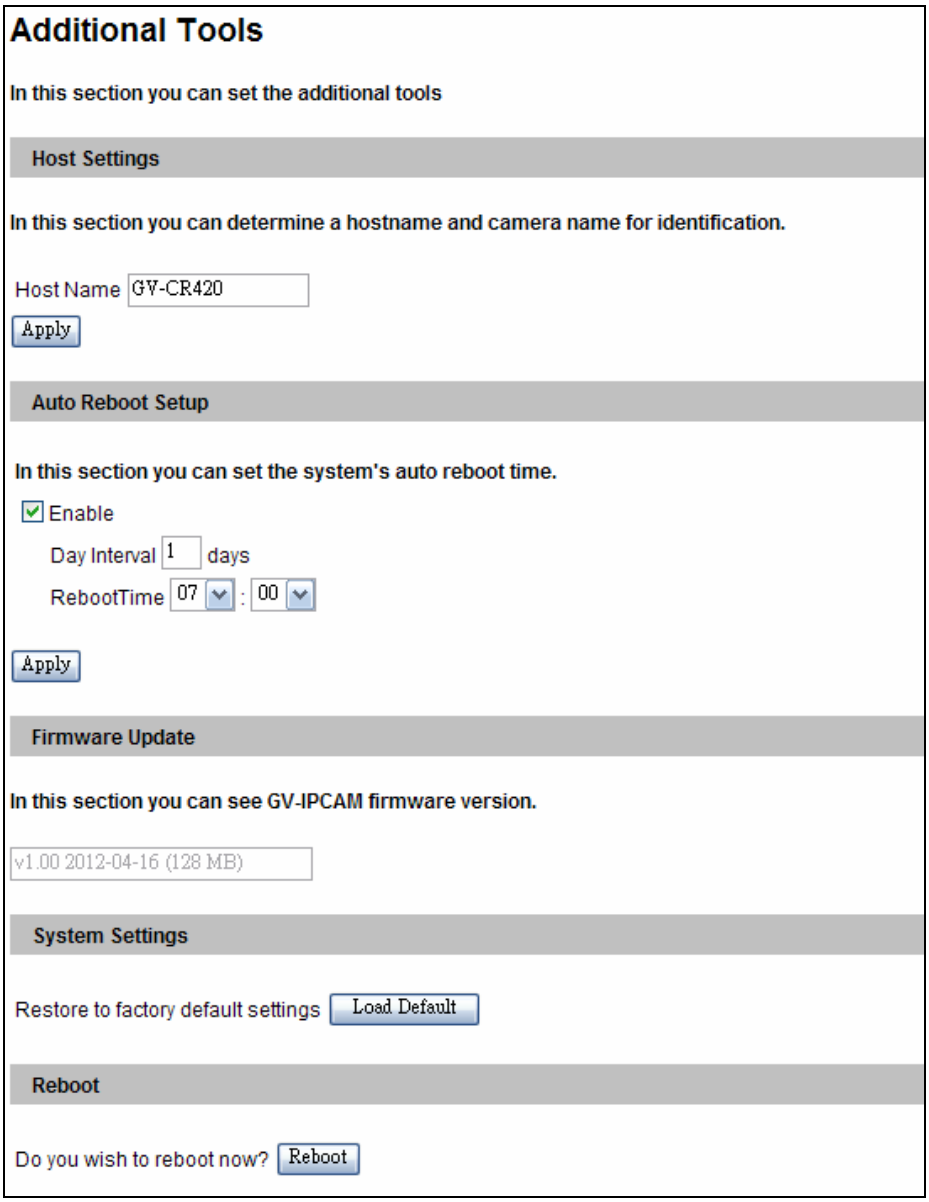

Additional Tools
In this section you can set the additional tools
Host Settings
In this section you can determine a hostname and camera name for identification.
Host Name GV-CR420
Apply
Auto Reboot Setup
In this section you can set the system's auto reboot time.
Enable
Day Interval 1 days
RebootTime 07 : 00
Apply
Firmware Update
In this section you can see GV-IPCAM firmware version.
v1.00 2012-04-16 (128 MB)
System Settings
Restore to factory default settings Load Default
Reboot
Do you wish to reboot now? Reboot

Figure 5-26

[Host Settings] Type a descriptive name for the camera.

[Auto Reboot Setup] Select **Enable** to activate automatic reboot and specify the time for reboot in the sub fields.

- **Day Interval:** Type the day interval between each automatic reboot.
- **Reboot Time:** Use the drop-down lists to specify the time for automatic reboot.

[Firmware Update] This field displays the firmware version of the camera.

[System Settings] Clicking the **Load Default** button will restore the camera to factory default settings.

Note: After applying the default function, you will need to configure the camera's network setting again.

[Reboot]

Clicking the **Reboot** button will make the camera perform software reset.

Chapter 6 Advanced Applications

This chapter introduces more advanced applications.

6.1 Upgrading System Firmware

GeoVision periodically releases the updated firmware on the website. The new firmware can be simply loaded into the camera using the Web interface or the **IP Device Utility** included on the Software DVD.

Important Notes before You Start

Before you start updating the firmware, please read these important notes:

1. If you use the IP Device Utility for firmware upgrade, the computer used to upgrade firmware must be under the same network of the camera.
2. Stop monitoring of the camera.
3. Stop all the remote connections including Center V2, VSM, and RTSP.
4. Stop the connection to GV-System.
5. While the firmware is being updated, the power supply and network connection must not be interrupted.

WARNING: The interruption of power supply during updating causes not only update failures but also damages to your camera. In this case, please contact your sales representative and send your device back to GeoVision for repair.

---

6. Do not turn the power off for 10 minutes after the firmware is updated.
7. If firmware upgrade fails, you will need to restore the camera to the default settings. For details, see *6.3 Restoring to Factory Default Settings* in the User's Manual.

6.1.1 Using the Web Interface

1. In the Live View window, click the **Show System Menu** button (No. 8, Figure 4-3) and select **Remote Config**. This dialog box appears.

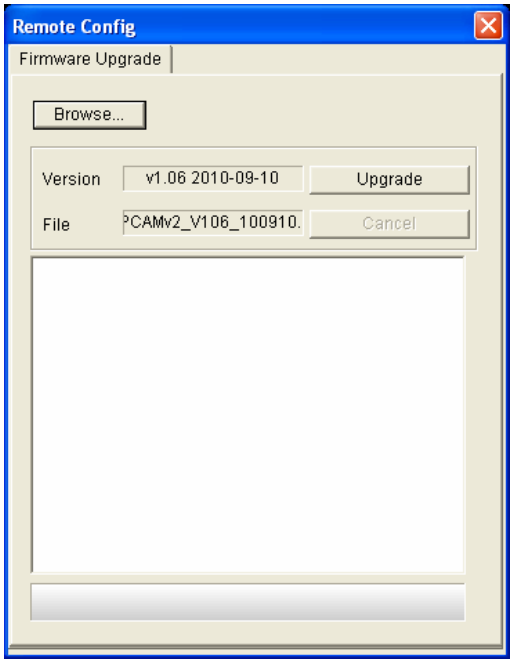


Figure 6-1

2. Click the **Browse** button to locate the firmware file (.img) saved at your local computer.
3. Click the **Upgrade** button to process the upgrade.

6.1.2 Using the IP Device Utility

The IP Device Utility provides a direct way to upgrade the firmware for multiple cameras. Note the computer used to upgrade firmware must be under the same network of the camera.

1. Insert the Software DVD, select **IP Device Utility**, and follow the onscreen instructions to install the program.
2. Double-click the **GV IP Device Utility** icon created on your desktop. This dialog box appears.

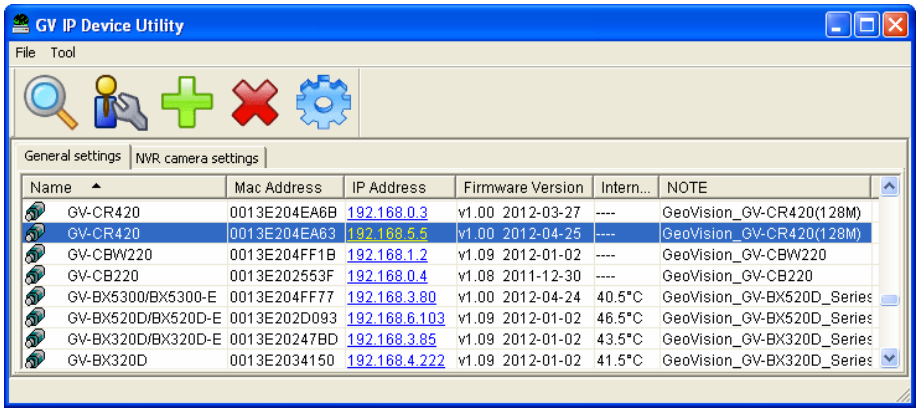

GV IP Device Utility
File Tool
General settings
NVR camera settings
Name
Mac Address
IP Address
Firmware Version
Intern...
NOTE
GV-CR420 0013E204EA6B 192.168.0.3 v1.00 2012-03-27 ---- GeoVision_GV-CR420(128M)
GV-CR420 0013E204EA63 192.168.5.5 v1.00 2012-04-25 ---- GeoVision_GV-CR420(128M)
GV-CBW220 0013E204FF1B 192.168.1.2 v1.09 2012-01-02 ---- GeoVision_GV-CBW220
GV-CB220 0013E202553F 192.168.0.4 v1.08 2011-12-30 ---- GeoVision_GV-CB220
GV-BX5300/BX5300-E 0013E204FF77 192.168.3.80 v1.00 2012-04-24 40.5°C GeoVision_GV-BX520D_Series
GV-BX520D/BX520D-E 0013E202D093 192.168.6.103 v1.09 2012-01-02 46.5°C GeoVision_GV-BX520D_Series
GV-BX320D/BX320D-E 0013E20247BD 192.168.3.85 v1.09 2012-01-02 43.5°C GeoVision_GV-BX320D_Series
GV-BX320D 0013E2034150 192.168.4.222 v1.09 2012-01-02 41.5°C GeoVision_GV-BX320D_Series

Figure 6-2

3. Click the **Search** button to locate the available cameras on the same LAN. Or click the **New** button and assign the IP address to locate the camera over the Internet. Or highlight a camera in the list and click the **Delete** button to remove it.
4. Double-click a camera in the list. This dialog box appears.

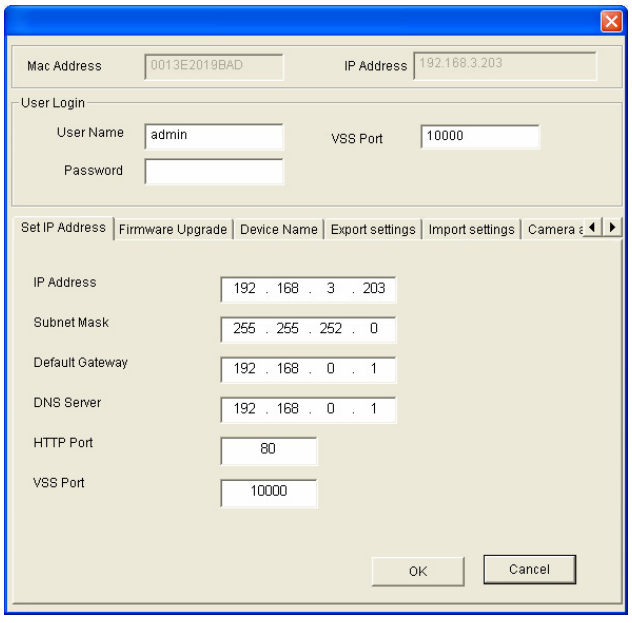


Figure 6-3

5. Click the **Firmware Upgrade** tab. This dialog box appears.

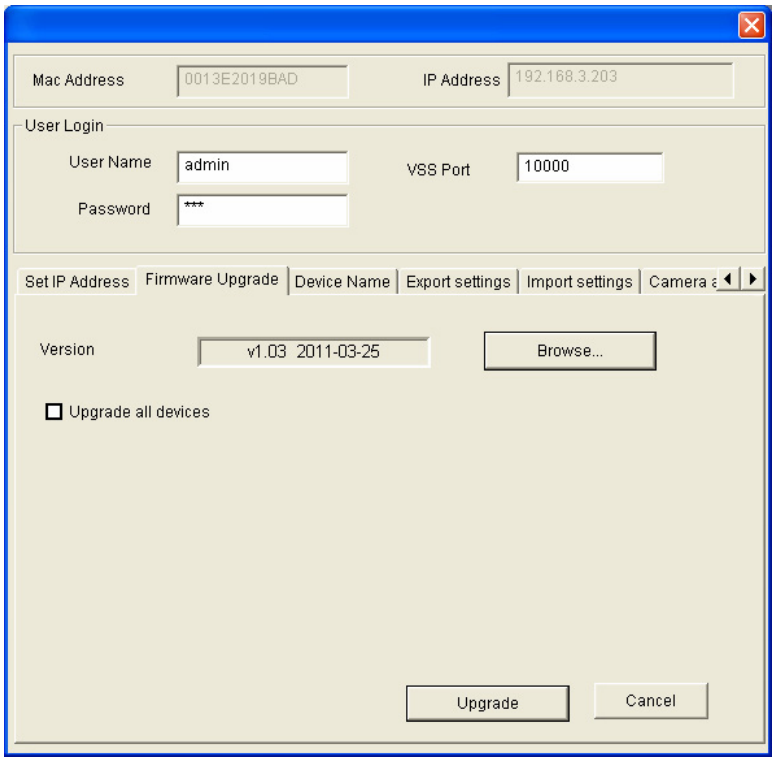


Figure 6-4

6. Click the **Browse** button to locate the firmware file (.img) saved at your local computer.
7. If you like to upgrade all cameras of the same model in the list, check **Upgrade all devices**.
8. Type **Password**, and click **Upgrade** to process the upgrade.

6.2 Backing Up and Restoring Settings

With the IP Device Utility included on the Software DVD, you can back up the configurations in the camera, and restore the backup data to the current unit or import it to another unit.

6.2.1 Backing Up the Settings

1. Run **IP Device Utility** and locate the desired camera. See Steps 1-3 in *6.1.2 Using the IP Device Utility.*
2. Double-click the camera in the list. Figure 6-3 appears.
3. Click the **Export Settings** button. This dialog box appears.

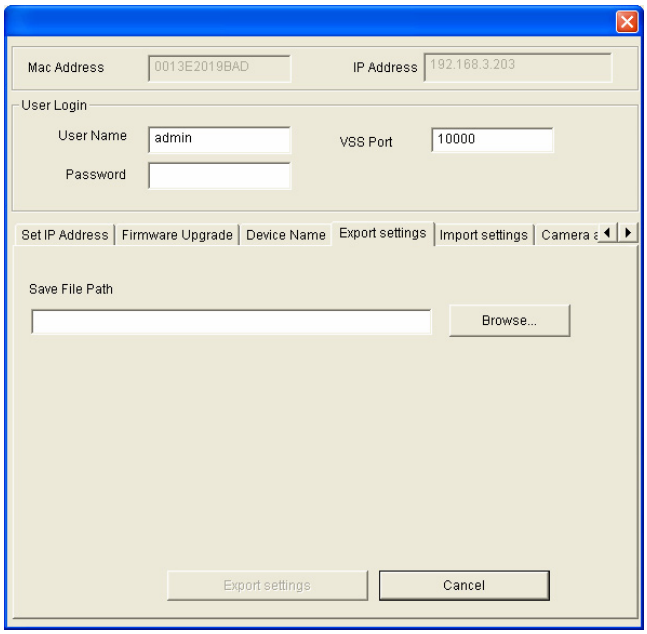


Figure 6-5

4. Click the **Browse** button to assign a file path.
5. Type the **Password**, and click **Export Settings** to save the backup file.

6.2.2 Restoring the Settings

1. In Figure 6-3, click the **Import Settings** tab. This dialog box appears.

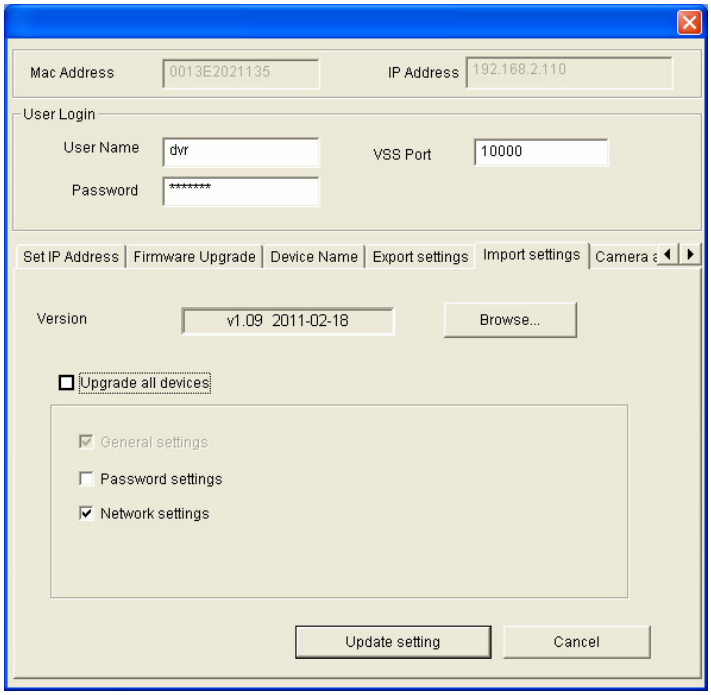


Figure 6-6

2. Click the **Browse** button to locate the exported file (.dat).
3. Select **Upgrade all devices** to apply the settings to all devices of the same model in the same LAN. To import password settings and/or network settings, select **Password Settings** and/or **Network settings**.
4. Click the **Update Settings** button to start restoring.

6.3 Restoring to Factory Default Settings

You can restore the camera to factory default settings using the Web interface or directly on the camera.

To restore to default settings using the Web interface:

1. In the left menu, select **Management** and select **Tools**.
2. Under the **System Settings** section, click the **Load Default** button.

To restore to default settings directly on the camera reader:

1. Unplug the power cable.
2. Use a pointy object such as the tip of a pen to hold down the **Load default** button (No. 8, Figure 1-3) while plugging the power cable.
3. Wait until the status LED blinks twice to release the **Load default** button. The process takes about 35 seconds.

6.4 Verifying Watermark

The watermark is an encrypted and digital signature embedded in the video stream during the compression stage, protecting the video from the moment of its creation. Watermarking ensures that an image is not edited or damaged after it is recorded. To enable the watermark function, see [Watermark], *5.1.1 Video Settings.*

The **Watermark Proof** is a watermark-checking program. It can verify the authenticity of the recording before you present it in court.

6.4.1 Accessing AVI Files

To verify watermark, first you have to access the recorded AVI files by one of these methods:

1. Use the **File Save** function on the Live View window (No. 3, Figure 4-3) to start recording on the local computer.

6.4.2 Running Watermark Proof

1. Install **Watermark Proof** from the Software DVD. After installation, a **WMProof** icon is created on your desktop.
2. Double-click the created icon. The Water Mark Proof window appears.
3. Click **File** from the menu bar, select **Open** and locate the recording (.avi). The selected recording is then listed on the window. Alternatively, you can drag the recording directly from the storage folder to the window.
4. If the recording is unmodified, a check will appear in the **Pass** column. On the contrary, if the recording is modified or does not contain watermark during recording, a check mark will appear in the **Failed** column. To review the recording, double-click the listed file on the window.

6.4.3 The Watermark Proof Window

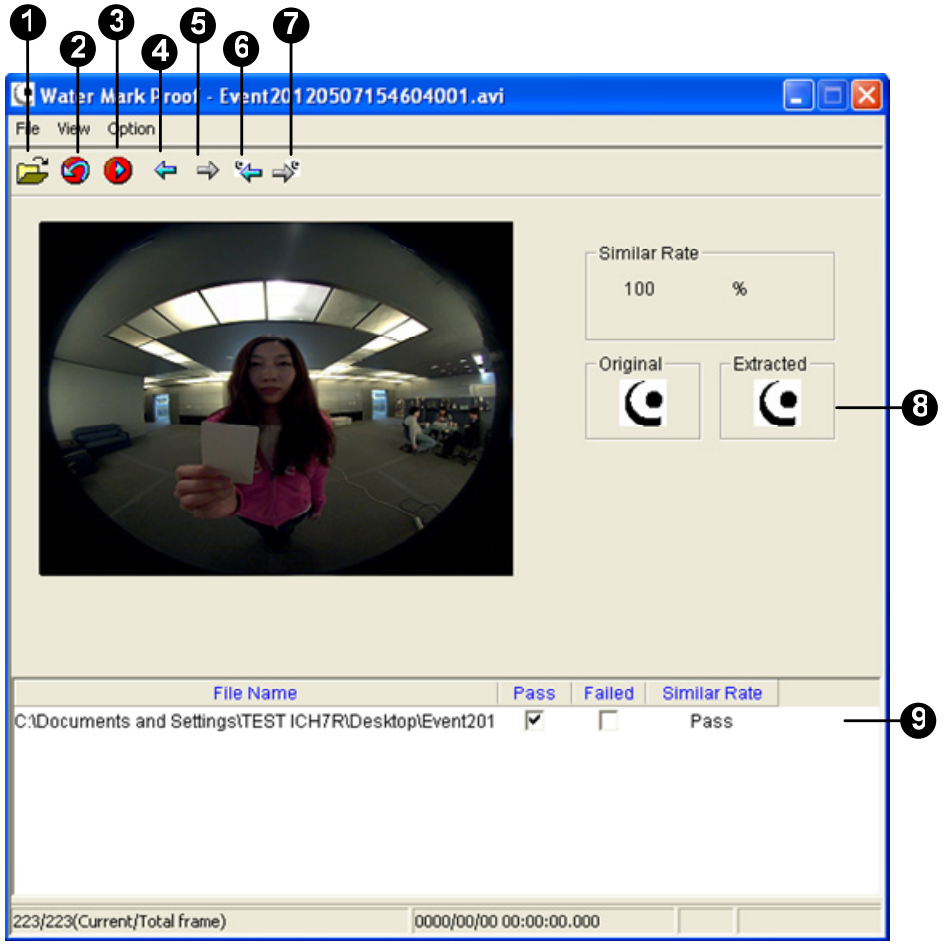


Figure 6-7

The controls in the window:

No.	Name	Description
1	Open File	Opens the recorded file.
2	First Frame	Goes to the first frame of the file.
3	Play	Plays the file.
4	Previous Frame	Goes to the previous frame of the file.
5	Next Frame	Goes to the next frame of the file.
6	Previous Watermarked Frame	Goes to the previous frame that contains watermark.
7	Next Watermarked Frame	Goes to the next frame that contains watermark.
8	Original vs. Extracted	The Extracted icon should be identical to the Original icon. If not, it indicates the recording has been tampered with.
9	File List	Displays the proof results.

Chapter 7 DVR Configurations

The GV-System provides a hybrid solution, integrating the digital videos from IP cameras with other analog videos. For digital videos, the GV-System provides complete video management, such as video viewing, recording, playback, alert settings and almost every feature of the system. The integration specifications are listed below:

1. The camera reader is compatible with GV-System **V8.5.4.0 or later**.
2. The maximum number of streams supported by the camera reader is **5**. When a camera reader is connected to IE browser or any other applications, it takes up **1** stream. When a camera reader is connected to GV-System, it takes up **2** streams.

Maximum number of streams	5
Connection from one GV-System	Takes up 2 streams
Connection to one GV-ASManager	Takes up 2 streams
One connection to Web interface	Takes up 1 stream
Connection from one Center V2	Takes up 1 stream

Note:

1. The above maximum numbers of streams are based on the maximum resolution for the camera and the codec H.264.
2. By default, the camera reader is in dual streams and will take up 2 streams when connected to GV-System.

3. The hardware compression and the “Pre-Recording Using RAM” feature cannot work on the videos from the camera reader.

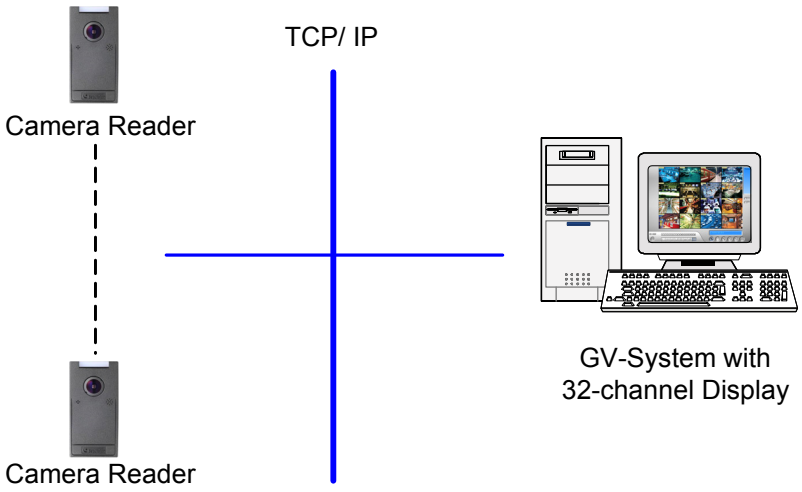


Figure 7-1

7.1 Accessing Camera View

To set up the camera reader and receive live view on the GV-System, follow these steps:

1. On the main screen, click the **Configure** button, select **System Configure**, select **Camera Install** and click **IP Camera Install**. This dialog box appears.

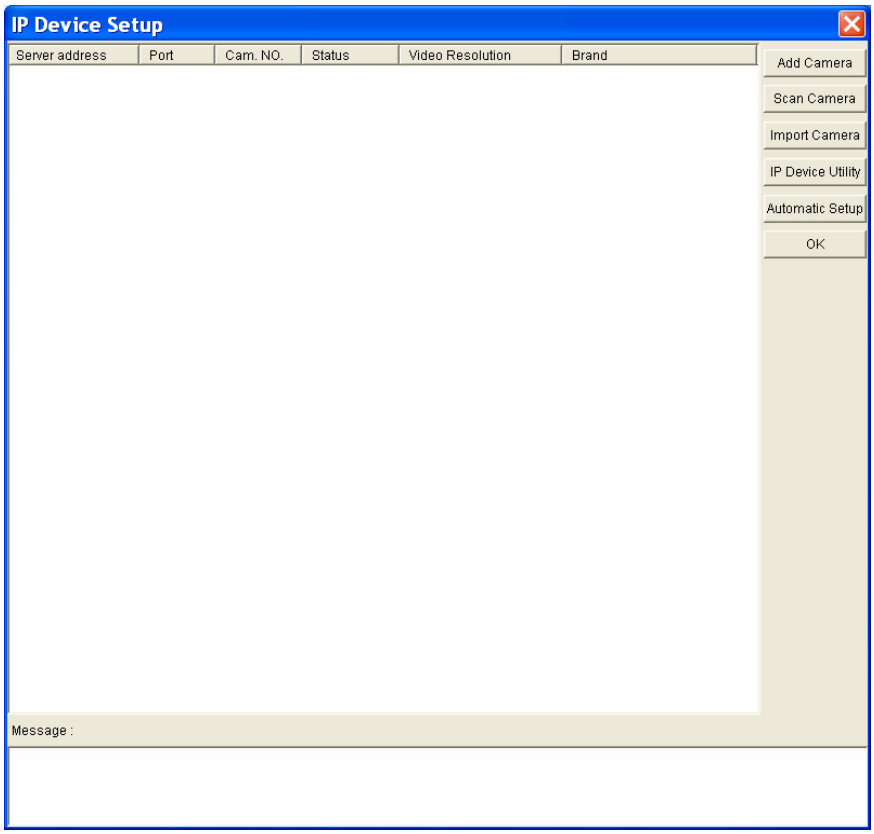


Figure 7-2

- To automatically set up the camera, click **Scan Camera** to detect any GV-IP devices on the LAN.
- To manually set up the camera, click **Add Camera**.

The following steps are the example of manual setup.

2. Click **Add Camera**. This dialog box appears.

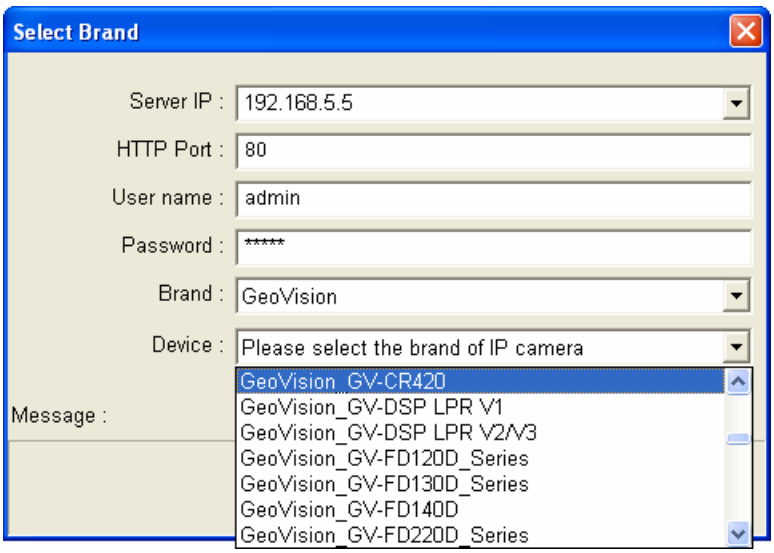


Figure 7-3

3. Type the IP address, username and password of the camera. Modify the default HTTP port if necessary. Select **GeoVision** from the **Brand** drop-down list and select the model from the **Device** drop-down list. This dialog box appears.

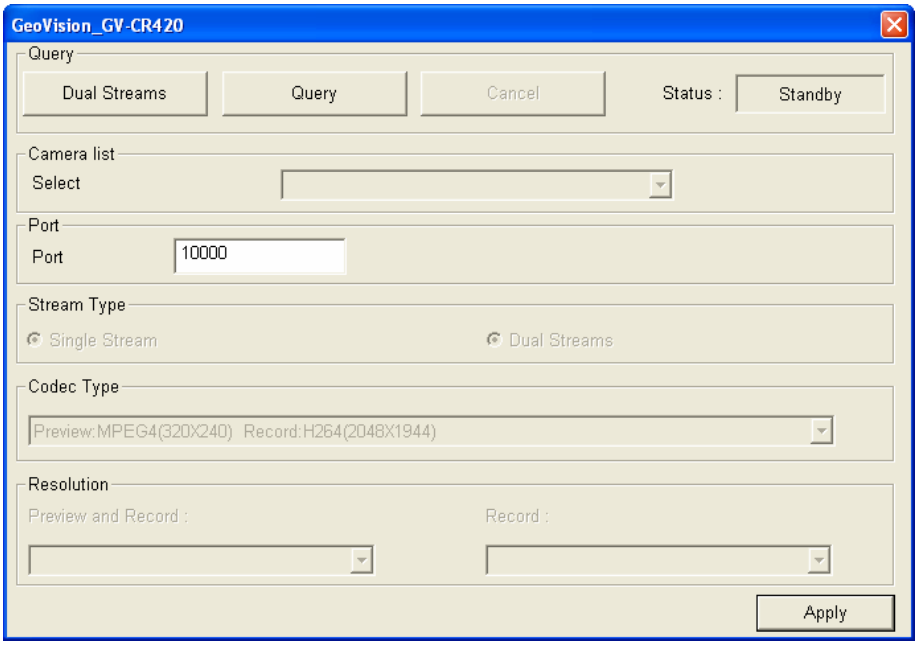


Figure 7-4

4. Click **Query** to acquire the information from the camera reader. The video streaming port should match the VSS port on the camera reader. The default port number is 10000.

5. Click **Apply**. The camera reader is added to the connection list.

6. Click the listed camera reader and select **Display position** to map the IP camera to a channel on the GV-System.

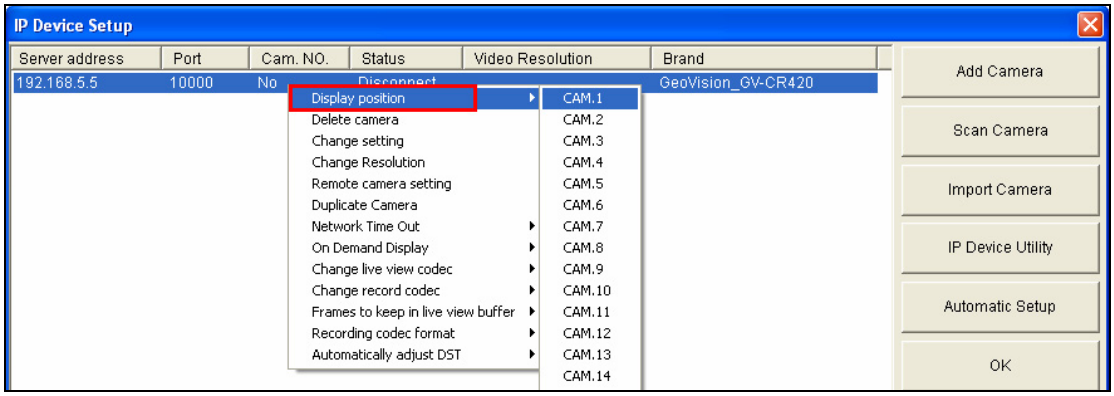


Figure 7-5

7. The Statue column should display “Connected”. Click **OK.**

7.1.1 Customizing the Basic Settings

After the camera reader is connected and assigned with a display position, you can configure the camera reader's settings such as frame rate, codec type and resolution. Right-click the desired camera reader to see the following list of options:

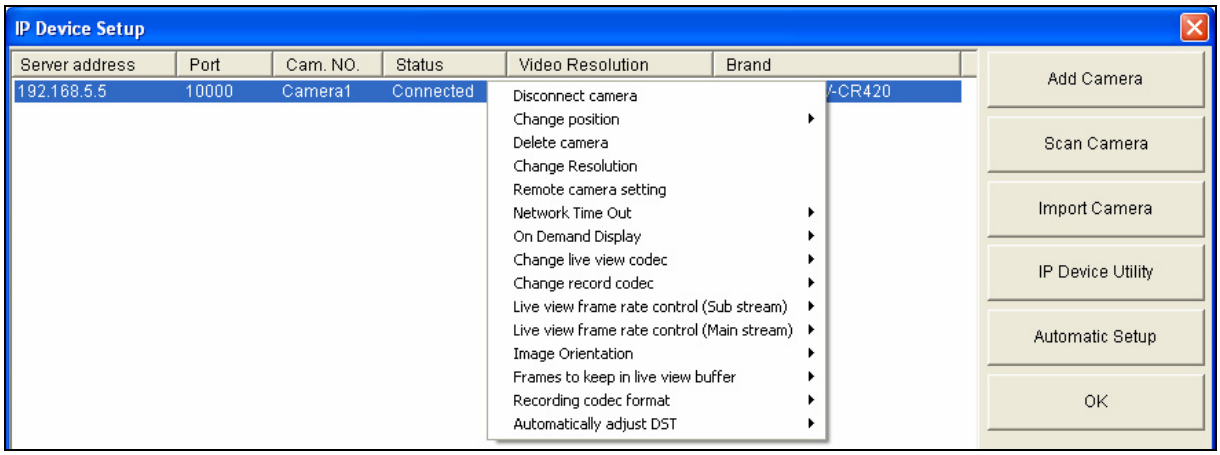


Figure 7-6

- **Remote Camera Setting:** Accesses the configuration interface of the connected device.
- **Network Time Out:** When network disconnection exceeds the specified time period, the camera status will be displayed as Connection Lost.
- **On Demand Display:** Enable automatic adjustment of live view resolution. Refer to the *On Demand Display* section in *DVR User's Manual* for more details.
- **Change live view codec:** Changes the code type of the live view.
- **Change record codec:** Change the codec type to record in.
- **Live view frame rate control (Sub stream):** Sets the live view of the sub stream to help reduce the CPU usage. If you have set the live view codec to be MJPEG, select the number of frames to allow in a second. If the live view codec selected is H.264, select one of the following options:

⊙ **Maximum Live-view Frame Rate:** View the video at the maximum frame rate possible.

⊙ **Live-view Key Frame only:** You can choose to view the key frames of the videos only instead of all frames on the live view. This option is related to the GOP setting of the IP camera. For example, if the GOP value is set to 30, there is only one key frame among 30 frames.

- **Live view frame rate control (Main stream):** Sets the live view frame rate of the main stream with higher resolution when On Demand function is enabled. Refer to the sub stream setting above to see the options available.

- **Image Orientation:** You can adjust the image orientation by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip** or **Rotate 180°**.
- **Frames to keep in live view buffer:** Specifies the number of frames to keep in the live view buffer.
- **Recording Codec Format:** Specifies whether to record in standard or GeoVision type of MJPEG H.264 codec.
- **Automatically Adjust DST:** If enabled, the time on the GV-IP device Web interface will be synchronized with the time of the GV-System when DST period starts or ends on the GV-System.

7.2 Receiving Card Numbers on GV-System

For GV-System to receive card numbers from the camera reader and overlay the data on live view, a physical connection between GV-System and the camera reader is required. Live view, on the other hand, is sent from the camera reader to GV-System through network connection.

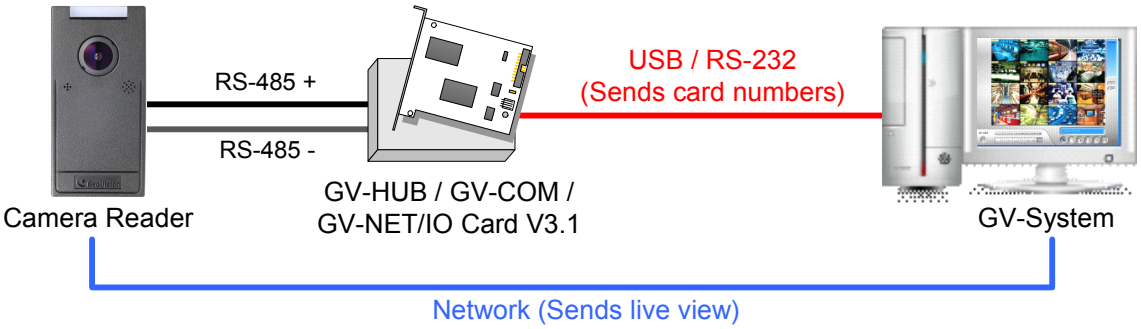


Figure 7-7

7.2.1 Defining ID Numbers for Multiple Camera Readers

When multiple camera readers are physically connected to GV-System, you will need to define an ID number for each camera reader. The ID number is used for mapping the card numbers to the correct live view channel. You will first need to connect the camera reader to a computer through GV-COM, GV-Hub or GV-NET/IO Card V3.1 in order to define an ID number.

Connecting the camera reader to a computer

To connect the camera reader to a computer, connect the camera reader to GV-COM, GV-Hub or GV-NET/IO Card V3.1 through RS-485 connection. Next, use an RJ-11 to USB cable or RS-232 to connect the GV-COM, GV-Hub or GV-NET/IO Card V3.1 to the USB port of the computer.

Defining ID for Camera Reader

1. Insert the software DVD and the Install Program window will pop up automatically.
2. Select **Install GeoVision USB Devices Driver**.
3. In the GeoVision USB Driver Installer window that appears, select **Install**.
4. Go back to the Install Program window, and select **Run GV-RK1352 Config Utility**. This dialog box appears.

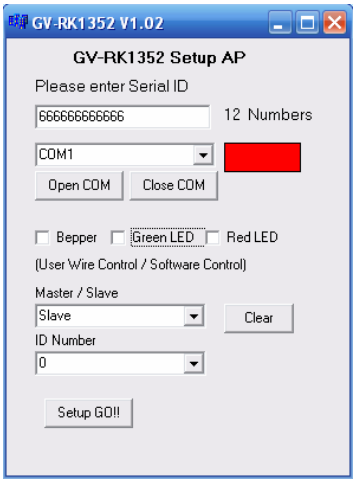
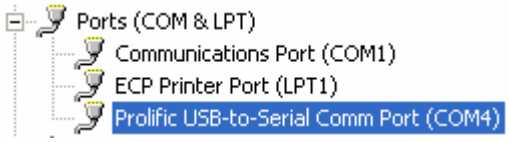


Figure 7-8

5. Type the barcode number of the camera reader in the Serial ID box. The barcode number is on back side of the camera reader.
6. Select the COM port that is connected to the camera reader and click **Open COM**. The red square next to the COM port box should change to blue if the COM port is correct.

Note: If the COM port is incorrect, an "***Error opening serial port***" message will appear. To verify the COM port that is connected to the camera reader, go to Windows Device Manager. In the Ports (COM & LPT) field, look for **Prolific USB-to-Serial Comm Port**. The COM port shown in parenthesis is the COM number currently in use.



---

7. In the Master / Slave drop-down list, select **Slave**.
8. Select an **ID number** for the camera reader. The ID number ranges from 0 to 7.
9. Click **Setup GO**. The settings are sent to the camera reader

7.2.2 Overlaying Card Numbers on Live View

To receive cardholder data on GV-System, connect the camera reader to GV-COM, GV-Hub or GV-NET/IO Card V3.1 through RS-485 interface and then connect the GV-COM, GV-Hub or GV-NET/IO Card V3.1 to the computer using a USB cable or RS-232 cable. Refer to *Figure 7-7*.

Follow the steps below to receive card number on GV-System:

1. On the main screen, click the **Configure** button, select **Accessories**, select **Camera Install** and click **GV-Wiegand Capture Device Setting**.
2. Click the **New** button. This dialog box appears.

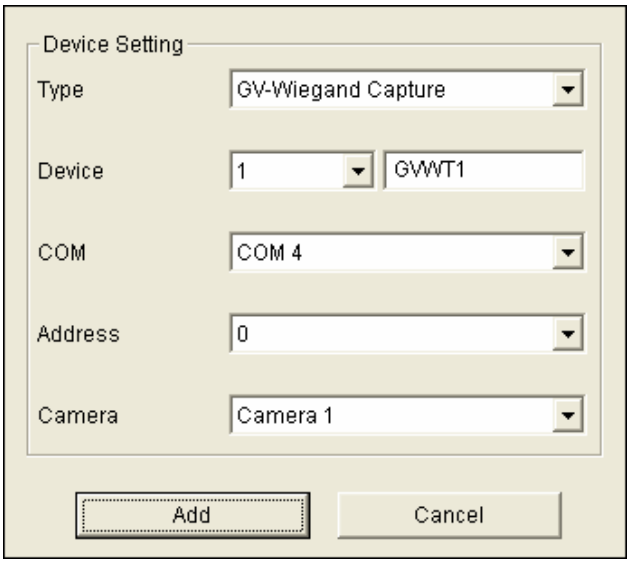


Figure 7-9

3. The following settings are available:
   a. **Type:** Select **GV-Wiegand Capture**.
   b. **Device:** Select a device number to identify the camera reader in System Log.
   c. **COM:** Select the COM port the camera reader is using.
   d. **Address:** If only one camera reader is connected, select the default ID number **0**. For multiple camera readers, select the ID number of the camera reader set in Config Utility.
   e. **Camera:** Select the channel of the camera reader to map the live view with the card number.
4. Click **Add**.

On the main page, the card number will now be overlaid on the live view when a card is presented. To adjust how the text is overlaid, refer to the *POS Data Overlay* section in *DVR User's Manual* for more details.

Chapter 8 CMS Configurations

This section introduces settings on connecting the camera reader in the central monitoring stations Center V2, VSM and Dispatch Server.

8.1 Center V2

The Center V2 can monitor and manage the camera reader.

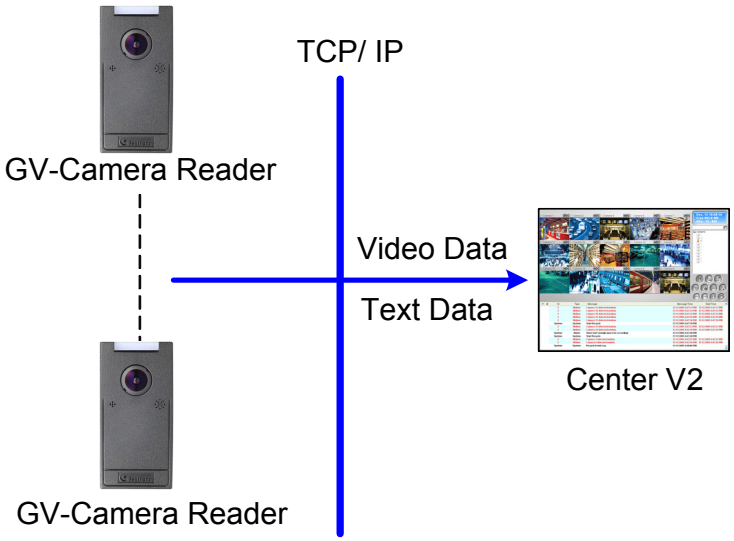


Figure 8-1

- To set the appropriate port for camera reader connection, click the **Preference Settings** button, select **System Configure**, click the **Network** tab, and check **Accept connections from GV-Compact DVR, Video Server & IP Cam**. Keep the default port **5551** for the Port 2 option, or modify it to match the Center V2 port on the camera reader.

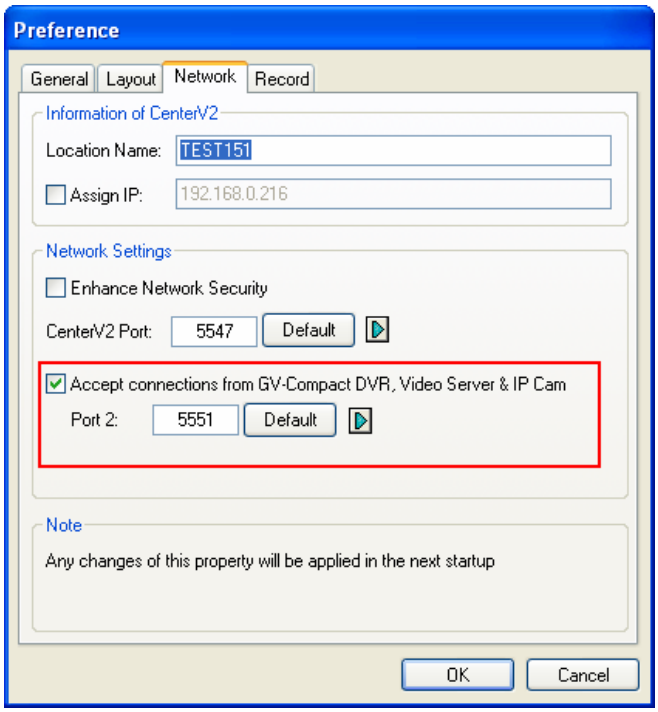


Figure 8-2

- To define how to display the received video on motion detection from the camera, click the **Preference Setting** button and select **System Configure**. This dialog box appears.

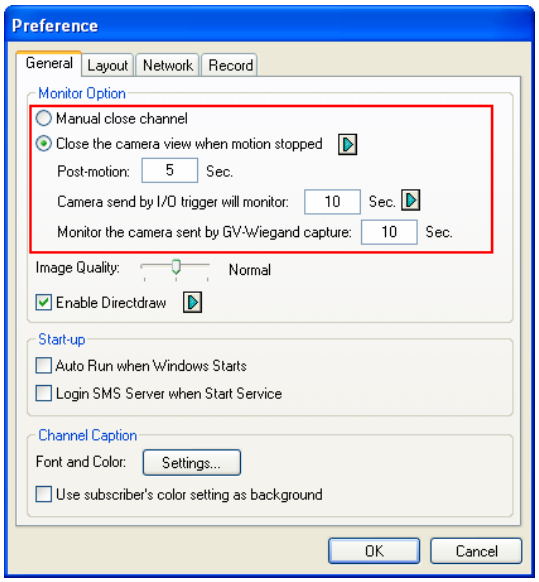


Figure 8-3

- **Manual close channel:** Closes the triggered camera view manually.
- **Close the camera view when motion stopped:** Closes the triggered camera view automatically when motion stops.
- **Post Motion:** Specify the duration of the camera view remaining on the monitoring window after motion stops.
- **Camera send by I/O trigger will monitor:** This function is not supported for GV-CR420.

To keep the camera view remaining on the monitoring window even after the alarm is finished, click the right-arrow button, and uncheck **Latch Trigger**. Then the camera view will keep remaining on the monitoring window for the specified time. For example, the alarm is triggered for 5 minutes and you set 10 minutes, which means the total display time will be 15 minutes.

For further information on how to manage the video received from the camera reader, see *GV-CMS Series User's manual.*

8.2 VSM

The VSM can monitor and manage the camera reader.

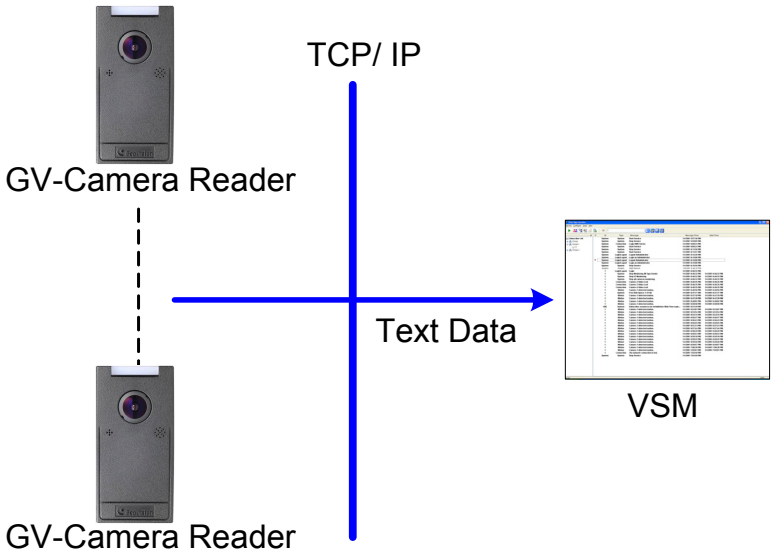


Figure 8-4

To set the appropriate port for camera reader connection, click **Configure** on the window menu, and select **System Configure** to display this dialog box. In the **Connective Port** field, keep the default value **5609** for the Port 2 option, or modify it to match the VSM port on the camera reader.

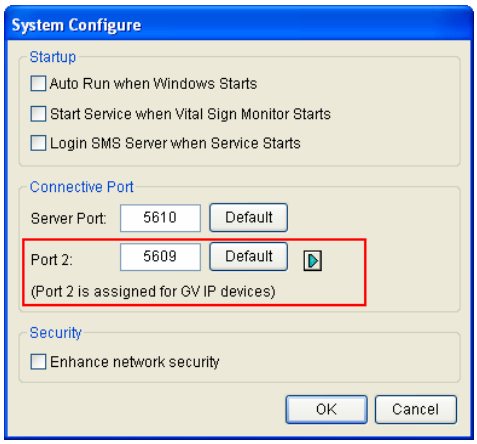


Figure 8-5

For further information on how to manage the video received from the camera reader, see *GV-CMS Series User's manual*.

8.3 Dispatch Server

The Dispatch Server minimizes overloading of Center V2 Servers by re-distributing camera reader subscribers to the least busy Center V2 Server.

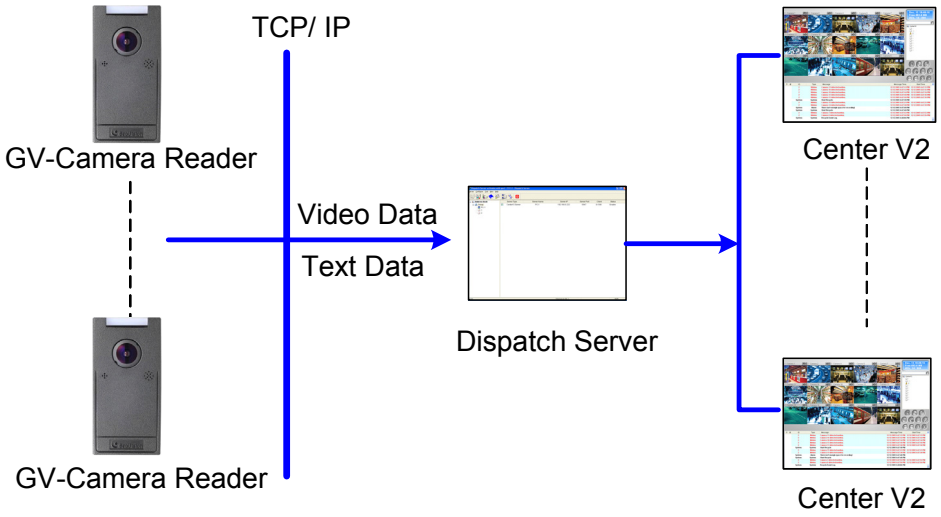


Figure 8-6

To set the appropriate port connecting to the camera reader, click the **Server Setting** button on the toolbar, and select **Allow GV IP devices to login as subscriber from port**. Keep the default port as **5551**, or modify it to match the Center V2 port on the camera reader.

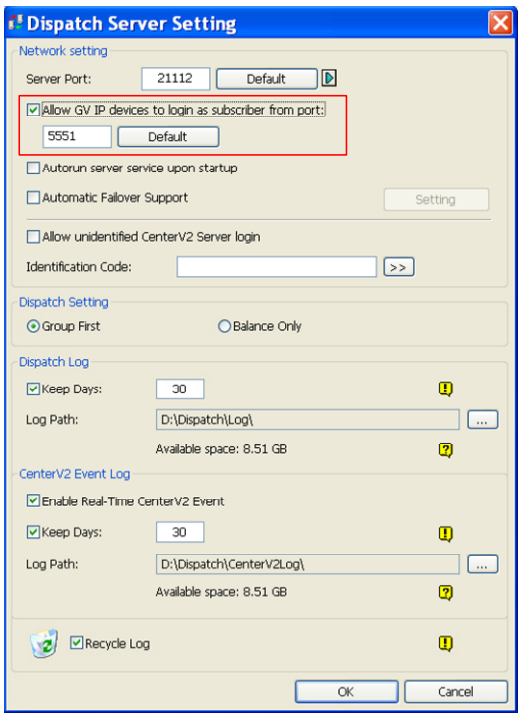


Figure 8-7

For further information on how to manage the video received from the camera reader, see *GV-CMS Series User's manual.*

Chapter 9 Mobile Phone Connection

Using iPhone, iPod Touch, iPad or Android Smartphones, you can now remotely connect to the camera reader to remotely watch live view and take snapshots

The latest information on GeoVision mobile applications is available at http://www.geovision.com.tw/english/5_4.asp

9.1 GV-Eye / GV-Eye HD for iPhone, iPod Touch and iPad

GV-Eye / GV-Eye HD allows you to connect to the camera reader from your iPhone, iPod Touch or iPad. GV-Eye is designed for iPhone and iPod Touch, while GV-Eye HD is designed for iPad.

System Requirements

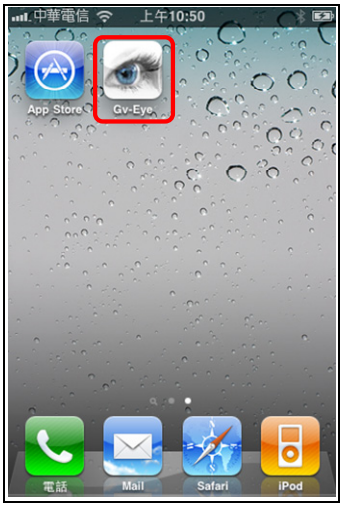
Handheld Device View	GV-Eye V1.2.1 for iPhone and iPod Touch GV-Eye HD V1.2.1 for iPad
OS Supported	iPhone OS 4.3.3 to 6.0.1
Port	VSS Port: 10000 (default)
Protocol	TCP/IP

Specifications:

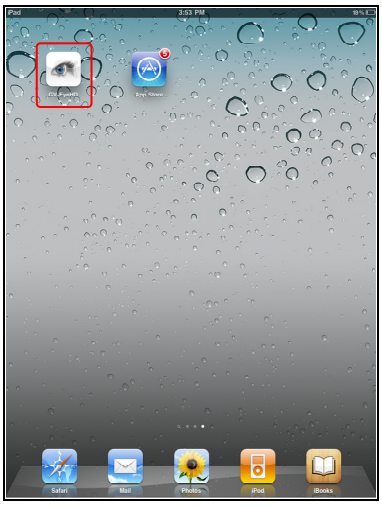
Supported Codec and Resolutions	**MJPEG**	2M (1920 x 1080) or lower
	H.264	2M (1920 x 1080) or lower
Supported Functions for CR420	Live View, Snapshots	
Note: GV-Eye can only access live view through stream 2 of the camera reader. Before connecting, make sure stream 2 is enabled on the camera reader Web interface.		

9.1.1 Installing GV-Eye / GV-Eye HD

You can download GV-Eye / GV-Eye HD from **App Store** and install the application. The GV-Eye / GV-Eye HD icon will appear on the desktop.



GV-Eye icon on iPhone / iPod Touch



GV-Eye HD icon on iPad

Figure 9-1

9.1.2 Connecting to the Camera Reader

To connect your iPhone, iPod Touch and iPad to the Camera Reader, follow these steps:

1. Click the **GV-Eye** icon on the desktop of your phone. The welcome page appears.
2. Tap the **Add** button . This page appears.

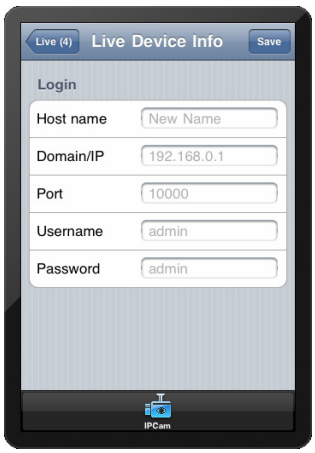


Figure 9-2

3. Type the Host name, Domain/IP address, port number (default value is 10000), username and password to log in to the camera reader.

4. Tap the **Save** button. The camera reader is now added to the connection list and will be available the next time you access GV-Eye.

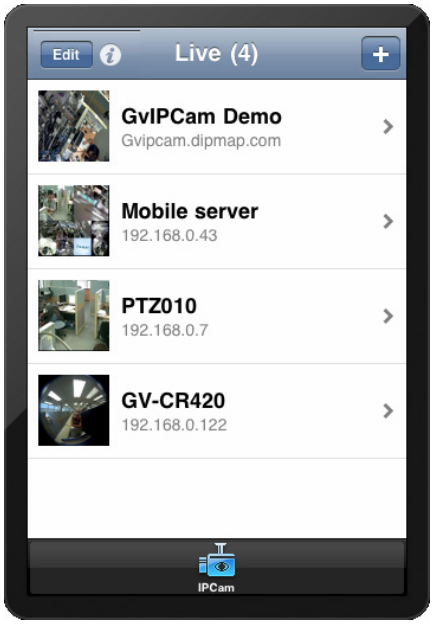


Figure 9-3

You can tap the **Edit** button Edit and then select the camera reader to edit existing login information. To delete login information, tap the **Edit** button and then tap the **Delete** icon . Tap the **Information** icon to access the installation guide.

5. Tap the host name to connect to the live view.

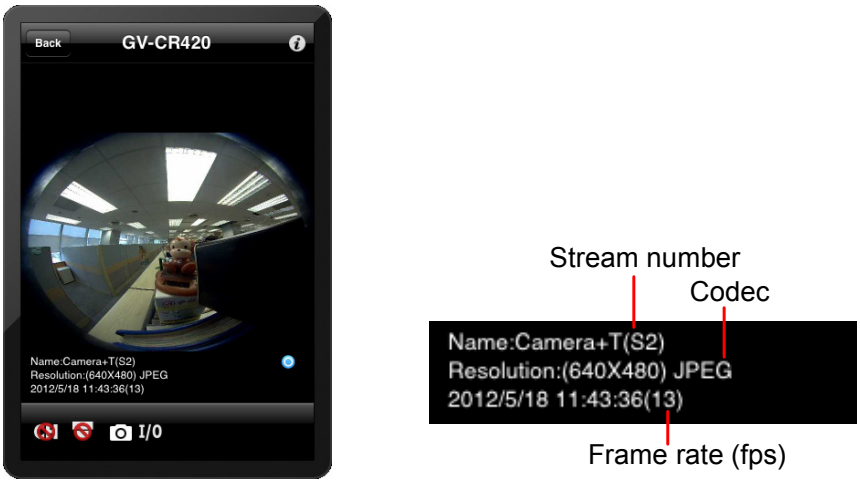


Figure 9-4

The buttons below are available when the iPhone, iPod Touch or iPad is positioned vertically.

Icon	Name	Function
	Snapshot	Saves the current image in the mobile device.
I/O	I/O Device	This function does not apply to GV-CR420.

9.2 GV-Eye for Android Smartphone and Tablet

With GV-Eye for Android, you can connect to camera reader using Android version 2.2 – 4.0 to remotely watch live view and take snapshots.

System Requirements

Handheld Device View	**GV-Eye V1.2.1 for Android Smartphones & Tablets**
OS Supported	Android version 2.2 – 4.0.2
Port	VSS Port: 10000 (default)
Protocol	TCP/IP

Specifications:

Supported Codec and Resolutions	**MJPEG**	2M (1920 x 1080) or lower
	H.264	2M (1920 x 1080) or lower
Supported Functions for CR420	Live View, Snapshots	
Note: GV-Eye can only access live view through stream 2 of the camera reader. Before connecting, make sure stream 2 is enabled on the camera reader Web interface.		

9.2.1 Installing GV-Eye for Android

Download **GV-Eye** from Android Market, and after installing the application, the GV-Eye icon will appear on the desktop.

Figure 9-5

9.2.2 Connecting to Camera Reader

To connect to the camera reader, follow these steps:

1. Tap the **GV-Eye** icon on the main page.
2. Tap the Menu button to access the following functions.

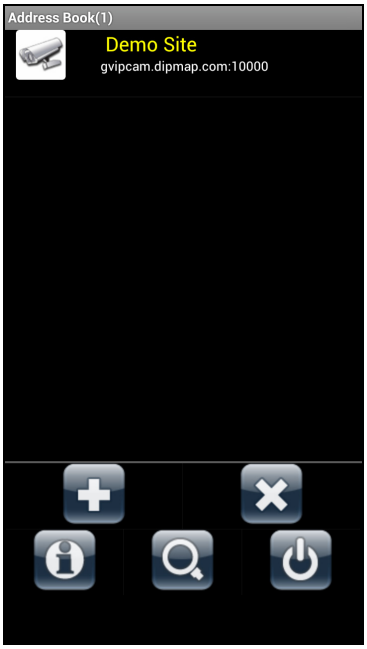


Figure 9-6

- **Add** the connection information of an IP device to the address book.
- **Delete all** entries in the address book.
- Displays the **Installation Guide**.
- Search IP Devices.
- **Exit** the application.

3. Tap the **Add** button , and then this page appears. Type the name, IP address, port number, user name and password of the camera reader.

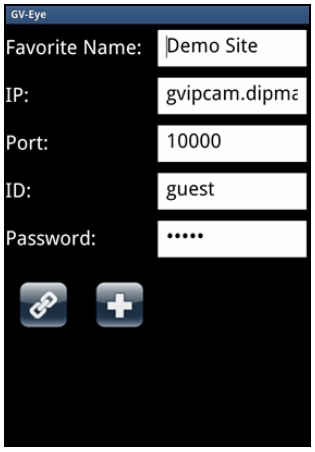


Figure 9-7

4. Tap the **Add** button to save the connection information to the address book.
5. Tap the created link in the address book.

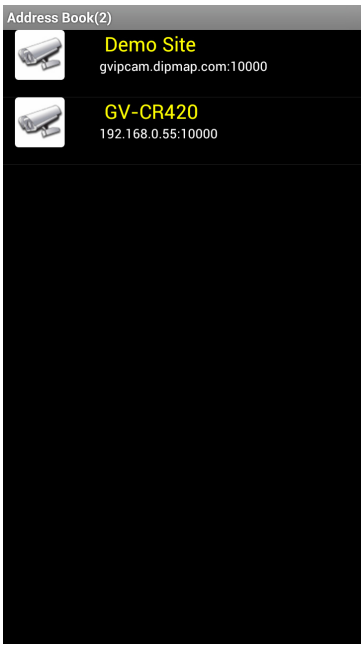


Figure 9-8

6. Tap the **Connection** button to access the camera reader.

9.2.3 Accessing Live View

You can press the menu button to see or hide the connection information.

The following function buttons are available:

Icon	Name	Function
	Snapshot	Saves the current image in the mobile device.
	Dual Stream	This function does not apply to GV-CR420.
	Screen division	This function does not apply to GV-CR420.
	Audio	Enables or disables the audio function. G.711 and G.723 audio codec are supported.
	PTZ Control	This function does not apply to GV-CR420.
	I/O Device	This function does not apply to GV-CR420.

Specifications

Camera

Image Sensor		1/2.5" progressive scan CMOS
Picture Elements		2048 (H) x 1944 (V)
Minimum Illumination	**Color**	4 Lux (1/30 sec), 2 Lux (1/5 sec)
	B/W	
Minimum Illumination for Face Detection		41-50 Lux
Shutter Speed		Automatic, Manual (1/5 ~ 1/8000 sec)
White Balance		Automatic, Manual (2800K ~ 8500K)

Optics Lens

Megapixel		Yes
Day / Night function		Yes (Electronic)
Lens Type		Fixed
Iris		Fixed Iris
Focal Length		1.05 mm
Maximum Aperture		F/2.8
Mount		M12, Pitch 0.5 mm
Image Format		1/2"
Angle of View	**Diagonal** **Horizontal** **Vertical**	185°
Operation	**Focus**	None
	Zoom	None
	Iris	Fixed
Note: Although GV-CR420 supports day / night function, they are not equipped with an IR-cut filter and therefore cannot work with infrared illuminators.		

Operation

Video Compression	H.264, MJPEG
Video Streaming	Stream 1 and 2 from H.264 and MJPEG
Video Resolution	2048 x 1944
Frame Rate	15 fps at 2048 x 1944
Image Setting	Brightness, Contrast, Sharpness, Saturation, Gamma, White Balance, Flicker-less, Backlight Compensation, Image Orientation, Shutter Speed, Day / Night, WDR, Defog
Audio Compression	G.711, AAC (16 kHz / 16 bit)

Network

Interface	10/100 Ethernet
Protocol	HTTP, HTTPS, TCP, UDP, SMTP, FTP, DHCP, NTP, UPnP, DynDNS, RTSP, PSIA, SNMP, QoS (DSCP), ONVIF

Mechanical

Lens Mounting		M12, Pitch 0.5 mm / 0.02 in
Connectors	**Power**	2-pin terminal block
	Ethernet	Ethernet (10/100 Base-T), RJ-45 Connector
	RS-485	2-pin terminal block
	Wiegand	2-pin terminal block
	Audio	Built-in microphone and speaker

Reader

CPU	8-bit RISC microprocessor
Frequency	13.56 MHz for ISO14443A (Mifare DESFire, Mifare Plus and Mifare Class)
Wiegand Interface	Wiegand 26 bit, distance 30 m / 98.43 ft
RS-485	9,600 bps, connect up to 8 GV-CR420 units
LED	Red, Green and Blue LED
Beeper	Buzzer

General

Operating Temperature	0°C ~ 40 °C / 32 °F ~ 104 °F
Humidity	10% to 90% (no condensation)
Power Source	12V DC, 0.35A
Maximum Power Consumption	15 W
Regulatory	CE, FCC, C-Tick, RoHS compliant
Dimension	134.6 x 42.5 x 65.8 mm / 5.3 x 1.7 x 2.6 in
Weight	170 g / 0.374 lb

Web Interface

Installation Management	Web-based configuration
Maintenance	Firmware upgrade through Web Browser or Utility
Access from Web Browser	Camera live view, video recording, change video quality, bandwidth control, image snapshot, audio, picture in picture, picture and picture, motion detection, privacy mask, tampering alarm, text overlay
Language	Bulgarian / Czech / Danish / Dutch / English / French / German / / Greek / Hebrew / Hungarian / Italian / Indonesian / Japanese / Norwegian / Lithuanian / Persian / Polish / Portuguese / Romanian / Russian / Serbian / Simplified Chinese / Slovakian / Slovenian / Spanish / Thai / Traditional Chinese / Turkish

Application

Network Storage	GV-NVR, GV-System, GV-Recording Server
Live Viewing	IE, GV-Multi View
CMS Server Support	GV-Control Center, GV-Center V2, GV-VSM

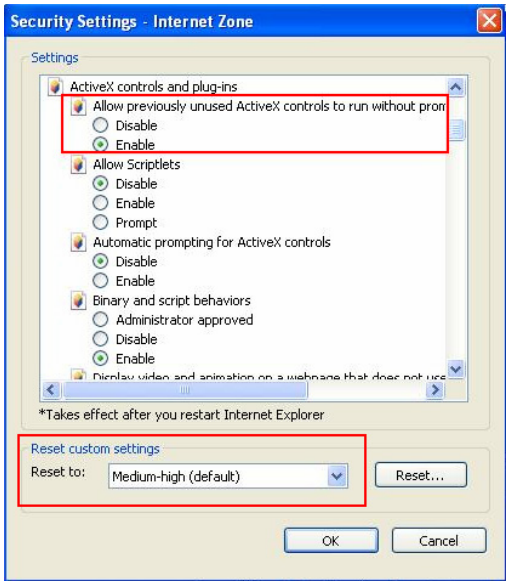
All specifications are subject to change without notice.

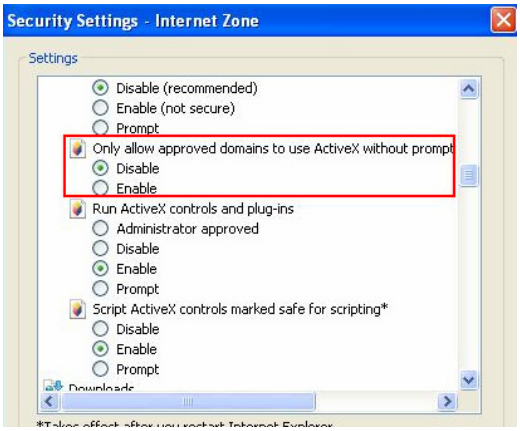
Appendix

A. Settings for Internet Explore 8

If you use Internet Explorer 8, it is required to complete the following setting.

1. Set the Security to **Medium-high (default)**.
2. Enable **Allow previously unused ActiveX controls to run without prompt**.
3. Disable **Only allow approved domains to use ActiveX without prompt**.





B. RTSP Protocol Support

The camera reader can support RTSP protocol for both video and audio streaming.

If you are using Quick Time player, use the following RTSP command:

rtsp://<IP of the camera reader>:8554/<CH No.>.sdp

For example, rtsp://192.168.3.111:8554/CH001.sdp

If you are using VLC player, use the following RTSP command:

rtsp://<ID>:<Password>@<IP of the camera reader>:8554/<CH No.>.sdp

For example, rtsp://admin:admin@192.168.3.111:8554/CH001.sdp

Note:

1. RTSP streaming is supported over HTTP, UDP and TCP.
2. The RTSP protocol must be enabled on the Web interface. See *4.3.8 RTSP*.
3. Only VLC and QuickTime players are supported for streaming video via RTSP protocol.

C. The CGI Command

You can use the CGI command to obtain a snapshot of the live view without logging in the Web interface or to access the User Account Web interface. For a camera reader with the following details:

IP address: 192.168.2.11

Username: admin

Password: admin

Desired stream: 1

Type the following into your web browser to **obtain a snapshot**:

http://192.168.2.11/PictureCatch.cgi?username=admin&password=admin&channel=1

Type the following into your web browser to **access the User Account Web interface**:

http://192.168.2.11/ConfigPage.cgi?username=admin&password=admin&page=UserSetting